

Using Identity Management to Achieve Security and Compliance

White Paper
January 2005



Table of Contents

Executive Summary	1
The Impetus for Change	1
The Role of Identity Management	2
Identity Management: Resolving the Contradictions Posed by Security and Compliance	3
Open, Yet Secure	3
Flexible, Yet Compliant	4
Effective, Yet Cost-Efficient	4
Sun Identity Management: Reducing Risk and Ensuring Compliance	5
A Comprehensive, Robust Approach to Security and Compliance	5
Sun Java™ System Identity Manager	5
Sun Java System Access Manager	6
Sun Java System Directory Server Enterprise Edition	6
Sun Java System Identity Auditor	6
Centralized Control for Secure Operations	6
Industry's Most Advanced Identity Auditing and Reporting	7
Cost-Efficient Implementation and Ongoing Operations	7
Security, Compliance, and Sun Identity Management: Two Case Studies	8
Transportation Case Study: Using Automated Identity Management to Increase Security and Lower Costs	8
Healthcare Case Study: Managing Complexity and Complying With Regulations	9
Your Business Runs Safer With Sun	10

Chapter 1

Executive Summary

At the turn of the twenty-first century, a unique convergence of world events and business trends propelled security and compliance to the forefront of concern for business enterprises and other organizations worldwide. Today, ensuring the security of sensitive information and achieving compliance with global regulatory requirements are among the most critical and, at the same time, the most daunting challenges facing any organization that hopes to operate successfully in today's increasingly open and global arenas. Identity management has emerged as a compelling solution for addressing both the technological and economic obstacles that threaten to thwart efforts to secure information and to comply with regulations.

The Impetus for Change

Ongoing developments on several major fronts are driving the need to achieve new levels of security and compliance today.

- First and foremost, the heightened risk to security and safety posed by terrorism affects every aspect of an organization's operations today. The risk extends not just to buildings and other physical assets but also to an organization's technological presence. For example, consider a breach in the secure information infrastructure of a defense contractor and the consequences that could follow.
- Ironically, the pressing need for more security comes at a time when technology infrastructures have become more difficult to secure than ever. The open exchange of information across organizational boundaries among diverse participants is unprecedented today. It's what enables a phenomenon like the virtual enterprise, with its promise of greater collaborative productivity than ever. But at the same time, it's also what endangers organizations in terms of opening them to higher levels of risk.
- The emergence of the virtual enterprise has given rise to increased concerns not only about safety but also about privacy. When multiple organizations and people are collaborating online, the potential for someone gaining unauthorized access to someone else's private or sensitive information is greater than ever.
- The pressure to comply with demands imposed by new regulations and legislation (such as the Sarbanes-Oxley Act, Gramm-Leach-Bliley (GLB) Act, Health Insurance Portability and Accountability Act (HIPAA), EU-IAS, Basel II, European Data Protection Act, BS 7799, and CA 1836) has increased as the result of two developments associated with more open collaboration. First, with the proliferation of electronic information in the age of the virtual enterprise, governments have stepped in to ensure the integrity and security of sensitive data as well as access to that data. Second, with the continued blurring of physical boundaries, organizations are becoming increasingly global in their operations, subjecting them to a more complex and diverse regulatory environment.

- Finally — and this is perhaps the greatest irony — stepped-up demands for more security and compliance have come about at the very same time as have economic pressures to do more with less resources. Meeting security and compliance demands must therefore be undertaken with an eye to cost savings and efficiencies at every turn.

The Role of Identity Management

Identity management can play a significant role in enabling organizations to meet today's demands for security and compliance. It is the only category of security-related and compliance-related technology that simultaneously enables centralized management of sensitive information and automates the processes that enable effective and efficient regulatory compliance. This paper describes in detail the challenges posed by security and compliance today, and how identity management enables organizations to meet them.

Chapter 2

Identity Management: Resolving the Contradictions Posed by Security and Compliance

One of the greatest challenges in achieving higher levels of security and compliance is in resolving the contradictions posed by the effort. The dilemma is: To collaborate productively, organizations must operate in environments that are open, yet tightly secured; flexible, yet stringently compliant; and effective, yet extremely cost-efficient. The following section looks at these requirements in more detail.

Open, Yet Secure

The Challenge: In the era of online collaboration, organizations and individuals can work together in ways that were unthinkable just twenty years ago. Today, companies are sharing data online with vendors for more efficient procurement. They are getting information from consumers electronically to enable convenient online transactions. They are storing supplier or customer data electronically to streamline operations and reduce costs. And those are just a few examples of the potential for profitable collaboration in the age of the virtual enterprise. Everywhere, organizations are joining with employees, partners, and suppliers to push the traditional boundaries of doing business.

That's the good news, but it's also the bad news. Doing business openly requires offering access to systems and information to an extent that is bound to pose risk. With so many more people and entities requiring access — and many of them operating outside the organization — the potential for unauthorized access is tremendous. Organizations that want to take full advantage of new possibilities for open collaboration must take precautions to also fully secure their systems and information. And, they must be able to track all access privileges and activity to ensure full compliance and address audit requirements while doing so.

The Solution: Identity management solutions that simultaneously support open standards and inclusionary security provide the type of open, yet secure infrastructure that extensive collaboration demands. This combination enables ongoing interoperability and consistent policy enforcement, creating an environment in which the potential for risk is minimized while the opportunity for collaboration is enhanced. The key characteristics of the open, yet secure environment are:

- A single point of control for managing identity throughout the user lifecycle
- Centralized visibility and control over access to critical systems and information to improve response time
- Ability to securely share identity data across trusted networks of partners, suppliers, and customers to create circles of trust in business-to-business (B2B) online networks

Flexible, Yet Compliant

The Challenge: The virtual enterprise by definition requires that participants be flexible — joining with a particular entity or entities for one purpose and then moving on to join with others for other purposes, as business or other requirements dictate. A shipping company, for example, may be part of a virtual enterprise as the supplier to a manufacturer that requires it to transport parts to physical facilities worldwide. The same company may also be part of a virtual enterprise as the supplier to a retail seller that uses it to deliver merchandise ordered online. The potential for the company's flexible involvement with others is virtually unlimited, and it must be able to flex and scale accordingly. At the same time, though, such an organization must also be able to comply with strict regulations that may govern its operations.

The more organizations (worldwide) with which an enterprise collaborates, and the more widespread its operations, the more complex the requirements for regulatory compliance will be — and the greater the costs for failing to comply. These costs may be as measurable and direct as large fines for failing a compliance audit, or as indirect as the loss of customer goodwill after private information has been compromised.

The Solution: To limit the risk of noncompliance and the costs that come with it, the right identity management solution must have robust capabilities for auditing and reporting as well as for flexibility and interoperability — easily integrating into an organization's existing IT infrastructure and delivering improved process improvements.

Effective, Yet Cost-Efficient

The Challenge: Instituting the infrastructure and capabilities to achieve open and flexible, yet secure and compliant, operations can be a significant undertaking. And because the stakes are so high, no corners can be cut — especially if doing so would undermine the effectiveness of efforts. The costs and difficulties associated with security and compliance are realized every day. To address the issues, organizations are adding staff, contracting with consultants, and implementing new processes — many of them manual and complex. Poorly executed plans can increase risk, potentially resulting in disastrous consequences such as millions of dollars in lost revenue and immeasurable losses in customer and partner confidence and loyalty. Yet today, IT departments are being asked to achieve these goals with less budget and fewer resources than ever before. Expenditures for technology to address these issues must represent high-value, truly strategic investments that deliver a measurable return — and do it fast.

The bottom line is that few companies can afford to pass up opportunities to do business more openly online; whether they pay the price in lost customers or government fines, the cost can be unthinkable. But what about the cost of taking advantage of those opportunities?

The Solution: The cost of being open, secure, and compliant need not be prohibitive. Identity management solutions that use automated processes to ensure openness, security, and compliance are essential to achieving both effectiveness and cost-efficiency in the era of the virtual enterprise. In fact, identity management can bring significant cost savings and competitive advantage to businesses that far exceed the benefits of being secure and compliant.

Chapter 3

Sun Identity Management: Reducing Risk and Ensuring Compliance

Sun identity management comprehensively addresses every aspect of security and compliance in a single set of solutions. Rather than having to piece together technology from multiple sources, enterprises can deploy an end-to-end approach to becoming more secure, compliant operations.

A Comprehensive, Robust Approach to Security and Compliance

Sun identity management solutions collectively address every aspect of identity management, from provisioning users to auditing and reporting on access activities.

Sun Java™ System Identity Manager

Java System Identity Manager provides integrated user provisioning and identity synchronization services for efficiently and securely managing identity profiles and permissions throughout the entire identity lifecycle.

Identity Manager provides automation of previously fragmented, manual processes for managing the full user lifecycle process. It greatly reduces the time it takes to:

- Get users up and running productively
- Change their access privileges as their roles change
- Instantly and securely revoke their accounts when their relationship with the company ends

Role- and rule-based provisioning provides the flexibility to set provisioning rules on users, organizations, resources, roles, or groups, ensuring that policies are enforced. Dynamic workflow supports multistep, complex provisioning and automates the process of making changes in identity data. Identity Manager also provides complete visibility into and control over user access privileges. A comprehensive and robust solution, Identity Manager lowers risk on multiple levels, improving security, audit performance, and legislative compliance.

Sun Java System Access Manager

Java System Access Manager is a security foundation that helps organizations manage secure access to Web applications — both within the enterprise and across B2B value chains.

Access Manager provides decentralized authentication and authorization services across internal and external computing domains and ensures that appropriate authentication credentials are required of users depending upon the value of the protected resources. It makes certain that authorized users have access to specific resources while protecting those resources from unauthorized users and presents streamlined navigation across enterprise Web applications through single sign-on capabilities. By offering single sign-on (SSO) as well as enabling federation across trusted networks of partners, suppliers, and customers, Access Manager secures the delivery of essential identity and application information to meet today's needs and to scale with growing business needs.

Sun Java System Directory Server Enterprise Edition

Java System Directory Server Enterprise Edition serves as the backbone to an enterprise identity infrastructure, enabling today's mission-critical enterprise applications and large-scale extranet applications to securely access consistent, accurate, and reliable identity data for significant operational and cost efficiencies.

Directory Server Enterprise Edition provides a solid foundation for identity management by providing a central repository for storing and managing identity profiles, access privileges, and application and network resource information. It integrates smoothly into multiplatform environments, and provides secure, on-demand password synchronization with Microsoft Windows Active Directory.

Sun Java System Identity Auditor

Java System Identity Auditor is the industry's first solution to make compliance-related activities a seamless part of everyday enterprise business by streamlining and automating the often manual and fragmented processes.

Identity Auditor enables organizations to have complete visibility into access privileges, facilitating adherence to key identity control objectives. Administrators can see at any time who has access to what information, receive immediate alerts about policy violations, and have remedial actions taken automatically. Identity Auditor also creates reports for review, provides a dashboard for visibility to current state, establishes an audit trail, and supplies readily available and auditable evidence of access events and privileges.

Open and integratable, all four solutions are designed expressly to reduce integration cost and complexity in the virtual enterprise.

Centralized Control for Secure Operations

Sun identity management solutions employ a variety of capabilities, features, and tools to ensure that access to sensitive information is subject to the most secure control possible. These capabilities include:

- Centralized visibility and control over access to critical systems and information
- A central point from which user accounts can be instantly revoked when the user's relationship with the organization has changed or ended
- The elimination of orphan accounts through active risk scanning of dormant accounts — accounts can then be eliminated, if necessary, to provide an accurate picture of the enterprise's activities
- Password management and policy enforcement to ensure the integrity of an enterprise's security program by restricting access to only authorized personnel

- Real-time insight into who has access to what resources and data at any given time
- Automatic detection of and response to potential risks such as dormant accounts
- Rule- and role-based access control to ensure that only appropriate levels of access to sensitive information are given to individuals based on their job functions and responsibilities
- Two-factor authentication technology for increased protection of high-value data
- Consistent enforcement of corporate security policies
- Directory proxy services that provide firewall-like protection against malicious attempts to compromise directory servers and act as a front end to prevent denial-of-service (DoS) attacks and access by unauthorized users

Industry's Most Advanced Identity Auditing and Reporting

To help enforce security policy, lower risk, and improve audit performance, Sun identity management solutions feature:

- Detailed information on user activity as well as the implemented controls
- Ongoing automated detection of violations of identity controls
- Streamlined, delegated verification of key identity controls
- Reports and audit trail for status or forensic purposes
- Auditable evidence of all activities
- Compliance reports for Sarbanes-Oxley, GLB, and HIPAA, as well as a number of other packaged reports to provide information on users' access activities

Cost-Efficient Implementation and Ongoing Operations

To reduce operational costs and speed the enterprise's return on its technology investment, Sun identity management technology:

- Automates the processes associated with improving security and achieving compliance, eliminating slow and costly manual processes
- Provides for repeatable delivery of identity information changes across multiple environments, including directories, eliminating the administrative burden of manual redelivery and repopulation
- Employs secure, delegated administration and user self-service capabilities to reduce administrative requirements and off-load the help desk

Chapter 4

Security, Compliance, and Sun Identity Management: Two Case Studies

Two large organizations representing diverse industries rely on Sun identity management solutions to ensure security and compliance.

Transportation Case Study: Using Automated Identity Management to Increase Security and Lower Costs

The Challenge: One of the largest railroad networks in North America needed to take steps to improve the security of its identity management processes — but without sacrificing operational efficiency. The solution had to be one that could handle an extremely widespread user population and a highly diverse application environment.

The Solution: The railroad chose Java System Identity Manager to manage identities and access privileges for users in hundreds of locations across North America. Identity Manager handles more than 100,000 user accounts for the railroad across a broad range of enterprise resources, including:

- IBM AIX
- IBM RACF mainframe security platform
- Microsoft Exchange Server
- Microsoft Windows 2000
- Microsoft Windows NT

The Technology: Identity Manager is a complete user provisioning and meta-directory solution for managing profiles and permissions securely and cost-efficiently. It is designed expressly to enhance security and, at the same time, lower costs through automated provisioning, threat detections, and other capabilities.

The Benefits: Rather than incurring significant costs to increase security, Identity Manager has instead generated significant savings. The railroad estimates that the automated identity management capabilities provided by the Sun solution have enabled cost reductions of more than 30 percent.

Healthcare Case Study: Managing Complexity and Complying With Regulations

The Challenge: A large U.S. pharmaceutical benefits services organization faced the triple challenge of managing identities securely in an increasingly complex environment, improving service to its clients and customers, and complying with new legislation governing access to sensitive patient data.

The Solution: The company uses Java System Identity Manager to securely and efficiently manage identities, accounts, and passwords for 12,000 employees, 1400 clients (insurance companies or payers), and 75 million patients. A broad range of managed resources in the enterprise includes:

- ACF2
- DB2
- IBM AIX and AS/400
- Infinium
- LDAP
- Lotus Notes
- Microsoft Exchange Server
- Microsoft Windows NT
- Oracle Financials
- SAP
- Sun's Solaris™ OS

The Technology: Identity Manager enables the company to operate securely and efficiently, and in compliance in an environment characterized by complexity. A high level of automation and data synchronization combine with other unique features to enable increased security and compliance as well as more efficient operations. Close control over who has access to sensitive data, as well as auditing and reporting capabilities, address the need to comply with the privacy protection requirements of the Health Insurance Portability and Accountability Act (HIPAA) and CFR 21 part 11.

The Benefits: The Company realized a 100-percent return on its investment in technology in just seven months and beat its target for internal rate of return by 20 percent. In addition, it has more than met its service-level agreement (SLA) requirements for provisioning clients. Finally, the technology has helped ensure the company's successful compliance with industry regulation requirements.

Chapter 5

Your Business Runs Safer With Sun

Security and compliance have taken on unprecedented importance today, and the price for failing to address them can be tremendous, from fines for noncompliance to customer ill will. Investing in the right identity management solution can be far less costly — and can even help to lower the cost of achieving security and compliance.

Sun identity management solutions offer a cost-effective, comprehensive approach to meeting today's vital security and compliance demands. Built on innovative technology, Sun identity management solutions address every aspect of secure identity management, from user provisioning and password management to access control and enterprise-wide auditing and reporting.

To learn more about identity management and its role in achieving improved security and compliance, or to request additional information about Sun identity management solutions, visit sun.com/identity_mgmt.

© 2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 USA

All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California.

Sun, Sun Microsystems, the Sun logo, [ADD APPLICABLE TRADEMARKS HERE] are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS HELD TO BE LEGALLY INVALID.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com



Sun Worldwide Sales Offices: Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323, Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45-4556-5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0, Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India-Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-67105-00, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +82-2-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100, The Netherlands +00-31-33-45-15-000, New Zealand-Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47-23-36-96-00, People's Republic of China-Beijing +86-10-6803-5588; Chengdu +86-28-619-9333, Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Saudi Arabia +9661-273-4567, Singapore +65-6438-1888, Slovak Republic +421-2-4342-9485, South Africa +27-11-256-6300, Spain +34-91-767-6000, Sweden +46-8-631-10-00, Switzerland-German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888, Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44 0 1252 420000, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800, or online at sun.com/store

SUN™ © 2005 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, and The Network is the Computer are trademarks, registered trademarks or service marks of Sun Microsystems, Inc. in the United States and other countries. Other brand and product names are trademarks of their respective companies. Information subject to change without notice. 01/05 R1.0