

The Business Case for Identity Management

A Business White Paper
September 2004



Table of Contents

The Shifting Landscape for Enterprise Application Access	1
Identity Management Delivers Value	3
Business Drivers for Identity Management	4
Building the Case: Operational Efficiency	5
Building the Case: Increased Security Effectiveness	6
Rapid Deployment = Rapid ROI	6
Internal Security Threats	6
Security Audits	7
Security in the Virtual Enterprise	7
To the Rescue: Identity Management	8
Reduced Development Costs	9
End-to-End Identity Management from Sun	10
Audit and Reporting	11
Conclusion	12

Chapter 1

The Shifting Landscape for Enterprise Application Access

For many — indeed, most — enterprises today, business strategy is increasingly predicated on the interdependence of processes among a broad array of participants. Those stakeholders now not only reach every corner of the business, but more importantly, they reach prospects, customers, partners, suppliers, consultants, contractors, and other vendors. The common foundation underlying all of these strategic business initiatives is “*a rapidly growing portfolio of enterprise IT applications.*” Today, the virtual enterprise is becoming a reality as companies furnish real-time access to sensitive enterprise IT resources, information, and applications to broadening constituencies.

- *Customer relationship management (CRM) systems* involve more users and departments, ranging from marketing to finance to customer service.
- *Enterprise resource planning (ERP) systems* manage the manufacturing and production processes. Supply chain initiatives synchronize the movements of materials and goods among upstream suppliers and downstream customers.
- *Human resources (HR) systems* enable employees to self-manage their benefit plans.
- *E-business systems* empower customers and partners to learn about products, see inventory, order products, and check order status.

The fact is, managing who accesses what resources is being shaped by several trends and factors.

- **Regulatory Compliance:** Thanks to legislative initiatives such as Sarbanes-Oxley, Gramm-Leach-Bliley, the Health Information Portability and Accountability Act (HIPAA), the European Union (EU) Directive on Data Protection, and others, information security is now a nonnegotiable mandate carrying stiff fines and even prison terms for noncompliance. Protecting the privacy of customers and patients as well as their sensitive personal information requires strict, process-driven management of IT application access to ensure that only those who have “need-to-know” access rights get to the information. And just as important is being able to report and audit access privileges and activity as needed. Unfortunately, many enterprises are trying to become compliant with manual and less efficient processes in order to ensure control.
- **User Diversity:** More than ever before, enterprise IT systems are being accessed by more and different types of users who require varying levels of access to different applications. They could belong to large groups, or they could be individuals with unique access requirements. They could be employees requiring long-term access, or they could be auditors needing access for only a week. The temptation is to apply a one-size-fits-all rule and group users into two or three broad categories, giving virtual *carte blanche* access to all but a few employees. It is fast, simple, inexpensive — and highly insecure.

- **Constant Change:** Just as important to note is that users' relationships with the company change. Employees are promoted and require different access privileges. The customer service representative who is promoted to sales now needs access to new sales-forecasting applications — and no longer needs access to previous applications. Temporary workers cycle through the company rapidly and must be provisioned and deprovisioned rapidly. Executives are transferred to other locations. A partner relationship ends and the partner now collaborates with your competition. This dynamic environment creates a steady stream of access privilege and basic identity data changes that must be administered.
- **Scalability:** Change can take place on a larger scale as well. New business models are requiring businesses to serve millions of customers daily. Mergers, acquisitions, divestitures, and reorganizations can drastically realign the dynamics of who accesses which IT resources. These events can require provisioning thousands or millions of users — whose productivity and satisfaction lags for every hour they are without access to mission-critical IT applications. Where workforce reductions are concerned, immediate deprovisioning is necessary as is being certain that all access points have been blocked permanently. The need for scalability also applies to the IT infrastructure. Where a directory designed for a mid-size company may meet present day needs, those requirements can escalate dramatically from an acquisition or change in business strategy that includes extranet collaboration.
- **Faster Provisioning:** Enterprises today typically have fragmented and manual processes for managing the full user lifecycle process, greatly increasing the time it takes to get users up and running productively, to change their access privileges as their roles change, and to instantly and securely revoke their accounts when their relationship with the company ends. One Sun customer — a large, global manufacturer — reduced its provisioning process timeline from two weeks after start date to two days prior. With an identity management solution from Sun in place, new employees are up and ready to go on their actual start date.

Ultimately, of course, access to a wider range of applications by a wider range of users can deliver game-changing benefits to the enterprise. Products ship faster. Costs are lower. Customer loyalty increases. Productivity climbs. However, broader access also presents significant obstacles. Administrators face the inherently conflicting challenges of managing rapid provisioning and deprovisioning, increasing information security, improving quality of service, streamlining processes, and, ultimately, reducing expenses.

The remainder of this paper will examine the challenges and business benefits associated with identity management — effective enterprise technology that enables an organization to capture, maintain, protect, analyze, and audit information about people interacting with the enterprise and manage the access rights, entitlements, privileges, and profile data of each user.

Chapter 2

Identity Management Delivers Value

Until recently, an IT investment in security solutions has sometimes resembled an insurance policy. It doesn't typically receive the highest priority for funding; however, if an organization ever suffers a security breach or an attempted intrusion, that investment rapidly pays for itself in a variety of ways by preventing or mitigating data theft (known, or worse, unknown), financial losses, embarrassing publicity, declining customer confidence, and more. In other words, the benefit was achieved by what didn't happen.

Identity management certainly provides these pain-avoidance benefits. However, it also can transform security and IT infrastructure from a necessary overhead cost to a potential source of significant and compelling payback. This radical shift comes just as business needs it most, when shrinking budgets and thinning profit margins have made it critical to see a return on every dollar spent. Justifying identity management improvement projects is often easier than many other security projects due to sheer efficiency gains.

Chapter 3

Business Drivers for Identity Management

There are a handful of business drivers that cause organizations to take action with an identity management solution. Unfortunately, these drivers may conflict with one another — causing pressure on the enterprise.

Starting with business and security objectives, technology has enabled new models for doing business with customers, partners, and even for offering better services to employees. There is a tremendous desire to take action where there is an opportunity for differentiation. However, this goal for more connectivity (opening up the business) only adds to the already increasing pressure for minimized risk to the organization because it means that IT resources are being accessed by a growing number and greater variety of users.

Similarly, cost reduction directives continue to be mandated. Opportunities for cost reduction come from looking at where operational efficiencies — for existing processes within a group, such as IT, or across groups, such as IT security, HR, purchasing — can be achieved, for example, how to offload spiraling help desk costs, how to recapture dollars by effectively turning off recurring charges for nondigital assets, or how to take advantage of HR investments to automatically drive what accounts and assets an employee is given. Since cost reduction often means having to do more with less, it can easily seem that cost-reduction tactics are in conflict with other directives that push for improved quality of service — whether it is improved employee connectivity or higher service levels for partners and customers.

Finally, in addition to these conflicting pressures, an overarching pressure is government regulations, which leave companies with no choice other than to look for solutions that aid their business processes so that they can prove compliance. In fact, now that penalties and jail time are realities, more companies are now taking action.

Chapter 4

Building the Case: Operational Efficiency

It is no secret that increasing access by more people to more applications creates a virtually unsustainable burden that IT must bear. The number of user accounts and levels of authorization create a mountain of low-value administrative work — work that carries a significant security risk if ignored or performed improperly.

Consider a company with 10,000 employees. The company also has partners and vendors who have varying levels of access to certain applications. A typical employee-user might have access to a half-dozen applications, such as network services, e-mail, HR benefits, and three enterprise applications. That holds true for new employees as well as those promoted or transferred to new responsibilities. External partners are likely to be limited to one or two applications. Even if it only takes five minutes to create a user account for each application, it quickly becomes apparent that the IT administrator in a company with a few thousand employees can spend dozens of hours every week simply creating or modifying access privileges. Password resets — the number-one source of help desk calls — can similarly occupy IT for many man-hours each week.

Just as important is the lost productivity of the users themselves. High-cost employees who are idle while awaiting access to new systems or awaiting a password reset present a largely hidden but significant expense as well.

With identity management, IT administrators can automate these manual, administrative processes for faster provisioning. The productivity increases on both sides of the equation — IT administrator and end user — are significant. Gartner estimates that a 50,000 user extranet environment can achieve a return on investment (ROI) of 310 percent and a savings of \$4 million — with a payback in just 7.5 months — from implementing an identity and access management solution.¹ Other ROI examples from implementation of identity and access management solutions range from 25,000 to 350,000 users, showing ROI from 90 percent to well over 110 percent.²

META Group found a similar rate of ROI solely through automating password resets. “In the 420 large organizations surveyed, respondents noted that automating password reset would reduce help desk calls by 30 percent. In a 10,000-user organization, this equates to \$648,000 annually.”³

Gartner also estimates that help desk calls cost an average of \$30 each, and that password management requests from users account for up to 40 percent of help-desk call volumes.

1. Gartner Webcast, September 2003.

2. Gartner Webcast, November 2003.

3. META Group: *Life-Cycle Management: Not Just for Security Anymore*, Chris King, META Group, June 17, 2002.

Chapter 5

Building the Case: Increased Security Effectiveness

While increased IT (and user) productivity can accelerate ROI or even totally cost-justify investments in identity management, these gains must not be achieved at the expense of effective security and compliance with legislative mandates. Those returns would be worthless if they exposed the organization to greater risk. And the risks are significant:

- Identity theft is becoming an increasingly prevalent goal of thieves.
- In a post 9/11 world, security threats include cyber terrorism.
- Insiders pose a serious threat, one that can cost an enterprise millions and result in a damaged reputation.
- New legislative and regulatory requirements for security improvements can impose stiff fines or penalties if not addressed.
- Providing access to extended enterprise users can compromise sensitive information.

Rapid Deployment = Rapid ROI

A major financial services company spent more than \$14 million over several years and estimated the need for \$45 million more over the subsequent 18 months to implement an identity management solution with a well-known software company. Scrapping that plan and implementing the Sun Java™ System Identity Manager in just 6 months, the company took advantage of Sun's flexible, agentless architecture and has met their requirements set by their board.

Internal Security Threats

Much of the expense and risk of security breaches stems from insiders who have at least some form of legitimate credentials — not from the hackers and external intruders. “Gartner estimates that more than 70 percent of unauthorized access to information systems is committed by employees, as are more than 95 percent of intrusions that result in significant financial losses. Add to that the mind-boggling potential for carefully planned crimes of mass destruction and you can see the temptation to impose rigid security measures.”⁴

4. *Security in a World Without Secrets*, R. Hunter, Gartner, February 2002.

The U.S. Treasury estimates that 60 percent of financial institution intrusions are committed by employees. From a cost perspective, these vulnerabilities can be very expensive. Aberdeen Group estimates that economic losses to consumers, businesses, merchants, credit issuers, and the financial industry would reach \$24 billion in 2003, compared to just \$8.75 billion in 2002.⁵ One of the chief contributors to this increased exposure is unmanaged user accounts, which the U.S. FBI cites as the second-highest cyber crime vulnerability.

Security Audits

Another key issue lies in the heightened profile of security audits. At a time when security has become of paramount concern to virtually every company in the world, the importance of security audits has increased accordingly. Security audits now command board-level attention, and information security and operations must be able to demonstrate the ability to control, audit, and report on which users have access to what information assets. Without this ability, they risk the possibility of a failed audit and its consequences. However, the audit is only an indication of the real risks the enterprise faces: Loss of proprietary information, productivity loss, even prison terms and fines can result from not addressing the issues identified by a security audit.

Security in the Virtual Enterprise

The virtual enterprise — the new standard of excellence for conducting business — creates an entirely new set of demands on IT organizations. It requires IT to not merely respond to change, but to anticipate and keep pace with it — at “the speed of business.” Those real-time changes could be market or product line expansions, new channels, mergers, acquisitions, or other restructurings. It is IT’s challenge to ensure that enterprise data, applications, and computing resources are quickly, easily, and appropriately accessible to new user communities. Effectively administering access privileges while maintaining security is key to building a successful virtual enterprise.

5. *2003 Predictions for Security and Privacy Report*, Aberdeen Group, January 7, 20003.

Chapter 6

To the Rescue: Identity Management

Identity management solutions enable IT administrators to effectively manage user permissions, privileges, and individual profile data required for the virtual enterprise. Identity management is all about controlling and automating the process that governs what each user has authorization to access. Through a range of features, identity management provides a centralized, single point of administration for provisioning and deprovisioning accounts as well as user self-service password management and access management, delegated administration for offloading responsibility to partners, and full auditing and reporting.

Ultimately, identity management provides what the enterprise needs: To capture, access, maintain, protect, analyze, and audit information about people. An identity management solution that is quickly and easily deployed speeds return on investment dramatically. The sooner an enterprise implements an effective solution, the sooner they can reduce costs of new user setups and password resets and begin to increase productivity and improve security. An effective identity management solution offers today's enterprise tremendous short- and long-term savings in a variety of areas, from the help desk to the security office.

A solution that can be rolled out rapidly enables the company to start reducing costs right away and recoup its investment in identity management much more quickly. Some of the significant savings an enterprise should expect to see include:

- **Efficient User Setup.** Significant reductions in the time required to set up new users or change user access levels leads to dramatic increases in productivity and lower costs.
- **Faster Processing of Requests.** Automation speeds the processing of requests, freeing security administrators to spend time on more productive activities.
- **Lower Help Desk Call Volumes.** With self-service password resets and single sign-on, users no longer have to call the help desk for assistance, eliminating many costly, time-consuming processes.
- **Improved Password Management.** Password synchronization streamlines password changes by applying them across multiple platforms and applications — all at the same time.
- **Improved Data Management.** Through implementation of a robust identity management infrastructure, data management efficiency is improved by greater than \$350/user/year.⁶
- **Lowered Support Costs.** Support costs are reduced as a centralized, high-performance, and scalable identity repository reduces troubleshooting time and error correction demands.

6. Giga Report, Giga Information Group, October 2002.

Reduced Development Costs

By centralizing identity information and making it consistently available to multiple applications instead of having each application store and maintain its own data in multiple locations, overall development costs are driven down significantly.

- **Increased Revenue Opportunities.** Faster deployment of an effective and scalable security model across all Web-based applications both within the enterprise and between business partners enables additional revenue flow.
- **Recouped Software Licensing Costs.** Organizations can save on software licensing costs by disabling dormant or inactive user accounts in a timely fashion and harvesting those licenses for new users.
- **Tighter Security.** Security costs can be reduced through access management, task automation, consistent policy application and enforcement, audit and reporting capabilities, and the ability to disable access at a moment's notice.

Chapter 7

End-to-End Identity Management from Sun

Focused on the most critical aspects of managing identities in today's complex enterprise environment, Sun provides the industry's most innovative and comprehensive solutions for identity management:

- **Sun Java System Identity Manager** is a noninvasive and secure user provisioning and data synchronization solution that uses automation and delegation to reduce the time and costs associated with enabling new users to start working productively and instantly disabling access when relationships change or end for a more secure enterprise. Java System Identity Manager also provides a complete password management solution that enables end users to manage their passwords themselves, increasing their satisfaction while greatly reducing associated support costs.
- **Sun Java System 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 on the value of the protected resources. Java System Access Manager makes certain that authorized users have access to specific resources while simultaneously protecting those resources from unauthorized users. It presents streamlined navigation across enterprise Web applications through single sign-on capabilities, and also enables the enterprise to audit all access activities, including authentication attempts, authorizations, and changes made, to assist in complying with regulatory audit requirements.
- **Sun Java System Directory Server Enterprise Edition** delivers secure, highly available, and scalable directory services for storing and managing accurate and reliable identity data. It serves as the backbone to an enterprise identity infrastructure, enabling today's mission-critical enterprise applications and large-scale extranet applications to access consistent, accurate, and reliable identity data for significant operational and cost efficiencies. Java System Directory Server Enterprise Edition integrates smoothly into multiplatform environments, and provides secure, on-demand password synchronization with Microsoft Windows Active Directory.

Audit and Reporting

Sun solutions include comprehensive identity auditing and reporting capabilities that prove essential to detecting security risks and dealing with them proactively.

- Identity Manager provides current and accurate reports of who is allowed access to what information and why, with the ability to adjust those access levels. Furthermore, reports reflecting changes to authorized access may be generated and automatically sent to managers at predefined intervals. This enables administrators to compare previous and/or current access records and make the changes necessary to preserve the required knowledge of accountability within the enterprise. Using Identity Manager, access data can be retained as long as necessary for the review of access history and user accountability. Access privileges related to specific dates can be recovered and studied for periodic reports or upcoming information security audits.
- Directory Server Enterprise Edition provides audit logging, which can be used to determine who accessed what and when. It also includes scripts that process these logs to create reports.
- Access Manager provides up-to-the-minute auditing of all authentication attempts, authorizations, and changes made. With real-time audit capability, Access Manager improves security and internal control by providing instant auditing of critical information.

Chapter 8

Conclusion

For enterprises that are grappling with administering access and authorization privileges for larger user populations, the challenges are daunting. There are the missed opportunities to provide superior customer service, achieve collaborative efficiency, and increase revenues. Just as important, identity management challenges translate into excessive costs from wasted help desk and IT resources as well as the lost productivity of users.

Regulatory compliance is also an increasingly prominent issue. Organizations that must comply with Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, the EU Directive on Data Protection, and similar legislation are under greater scrutiny to ensure that information stays secure — even in the face of competing legitimate demands for greater access. With the specter of lawsuits, criminal penalties, and boardroom visibility, identity management is more important than ever before.

Collectively, Sun solutions provide an end-to-end comprehensive identity management solution for companies that need to manage identity profiles and permissions in a manner that ensures the security of the enterprise, the accuracy of business transactions, and the privacy of users while greatly reducing the traditional costs of managing identities in an ad hoc manner.

For more information, 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, Java, and The Network is the Computer 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.



Please
Recycle



Adobe PostScript

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 +972-9-9710500, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +822-2193-5114, 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 +421-2-4342-94-85, 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 +44-1-276-20444, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800, or online at sun.com/store

SUN © 2004 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Java, and The Network is the Computer are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Information subject to change without notice. 09/04 R1.0