

ACCESS CERTIFICATION: ADDRESSING AND BUILDING ON A CRITICAL SECURITY CONTROL

White Paper
October 2008

Table of Contents

Executive Summary

The Forces Driving Security Controls Related to Access	1
Ongoing and growing pressure to prove compliance	1
Insider threats resulting from inappropriate access	1
Need to expand reach and manage risk	1
Using Access Certification to Address Critical Issues	2
Understanding, validating, and documenting access	2
Maintaining security within and beyond the enterprise	2
Laying a foundation for IAM initiatives to manage risk	3
Key Criteria for an Access Certification Solution	4
Comprehensive automation	4
Minimal customization and programming requirements	4
Integration with provisioning and role management	4
Depth of vendor expertise	5
Sun Identity Compliance Manager	6
Comprehensive capabilities	6
Easily integrated with existing infrastructures	6
Part of a complete portfolio of identity solutions	6
From the recognized leader in identity management	7
Identity Compliance Manager at Work in the Real World	8
Goal: Improve access certification	8
Conclusion	9

Executive Summary

Today's enterprise faces multiple, multi-faceted business challenges in which the management of employees' and partners' access to enterprise resources is vital. Foremost among these is the challenge of complying with an ever-growing number of regulations governing the integrity and privacy of enterprise data. With the need to protect data comes, of course, the need to closely manage access to it — by knowing at all times who has access to resources and whether their access is appropriate, and by providing documentation of this information in the event of an audit.

But compliance is not the only challenge in today's enterprise. Even more critical is the need to operate an agile business that can respond quickly and competitively to business opportunities and competitive threats. Operating such a business while remaining compliant is a tall order. To succeed, a company must have an identity and access management (IAM) infrastructure in place to ensure that people have access to all the resources they need (but none of those they don't), and to prove in audits that access is being managed correctly and in compliance with internal security policies and external regulations. Moreover, this infrastructure must be based on efficient and effective processes that free people to focus on the growth of the business without having to devote undue time and budget to its security.

This paper will examine these often conflicting demands on the enterprise and show how access certification technology makes it possible to meet them, first by enabling access control compliance, and second, by laying the foundation for a strong IAM infrastructure. It will:

- Describe the forces driving security controls related to access
- Explain how access certification addresses these issues
- Discuss the key criteria for an access certification solution
- Introduce Sun Identity Compliance Manager for access certification
- Present real-world examples of Sun solution deployments

Chapter 1

The Forces Driving Security Controls Related to Access

Ongoing and growing pressure to prove compliance

In the “alphabet soup” of regulations governing business around the world today, one of the most pressing concerns is the integrity and privacy of data. From Sarbanes-Oxley, with its emphasis on the integrity of financial information, to the Health Insurance Portability and Accountability Act (HIPAA) and other industry-specific laws protecting data privacy, regulations force companies to focus on access. They have specifically led to increased scrutiny of assigned access to enterprise systems, applications, and data. It is vital for companies to know — and even more important — to be able to prove who has access to what, whether that access is appropriate, and what is being done about it if it isn't.

Insider threats resulting from inappropriate access

The need to closely govern access to systems and resources extends beyond complying with regulations to protecting enterprise assets. The threat posed by inappropriate access is grave. One can look all the way back to the 1990s, when accounting fraud caused the collapse of Barings Bank and when unauthorized trading resulted in nearly \$2 billion in losses for the London Metal Exchange. And such problems have continued to proliferate; consider, for example, the 2008 Société Générale trading loss incident in which fraudulent transactions by an employee caused the bank to lose billions. Clearly, these insider threats must be eradicated — and an important step toward that is eliminating opportunities for inappropriate access to systems by rogue traders and other insiders.

Need to expand reach and manage risk

While security is critical to preventing business losses, it must be balanced against the openness that is equally critical to achieving business agility in the Web 2.0 era. Systems must be locked down to the extent that they keep out malevolent efforts to gain access from inside or from outside the enterprise. But at the same time, they must be open enough to ensure that everyone who is working in the best interests of the enterprise can get their jobs done. Open access must be coupled with access control to achieve this careful balance between agility and security. A business that is secure in its ability to appropriately control access to its resources will be empowered to apply those resources to bold and confident growth and expansion.

Chapter 2

Using Access Certification to Address Critical Issues

The forces described in the previous chapter are leading companies to take action to address the following:

- Understanding who has access to what systems, applications, and data
- Validating that the assigned access is correct and appropriate
- Documenting and providing evidence for both of the above

An automated access certification solution will enable the enterprise to address these issues and, in the process, maintain security and manage risk.

Understanding, validating, and documenting access

An effective technology solution for access certification can provide a clear and comprehensive understanding of who has access to what resources by automatically consolidating and correlating entitlement data from throughout the enterprise and reporting on user access across enterprise systems and applications. In addition, such a solution will speed and increase the accuracy of access review and validation through the use of automation.

An effective solution will also empower decision makers to revoke any inappropriate access that it detects so that the enterprise can enforce policies in areas such as separation of duties and least privilege. Finally, it will provide reports leveraging the resulting audit trail to provide evidence that assigned access has been reviewed and, where necessary, corrected.

Maintaining security within and beyond the enterprise

Access certification is critical to maintaining security, particularly in guarding against access violations that could lead to security breaches. Regularly scheduled access reviews ensure that users are assigned the appropriate minimum access necessary to do their jobs — and no more. Event-based access reviews that are triggered by transfers, promotions, or terminations ensure that internal employees do not aggregate access as they move throughout the organization and that both internal and external users do not retain access when their relationships with the organization end.

Laying a foundation for IAM initiatives to manage risk

Identity and access management is the cornerstone of an enterprise's ability to extend its reach while still managing business risk. Access certification technology lays the foundation for initiatives in this area in several ways. It accomplishes the fundamental work of consolidating and correlating identity and access data — the same data that can be used in provisioning and role management. The entire process of certification by its very nature “cleanses” the consolidated data, leaving an excellent foundation on which to build.

Chapter 3

Key Criteria for an Access Certification Solution

Comprehensive automation

An effective access certification solution should automate the entire certification process, from building a warehouse of entitlements, to scheduling and monitoring certifications, to providing ongoing tracking and reporting. The solution should have the functionality to automatically:

- Import entitlement data from the existing IT infrastructure and from any enterprise application, and to correlate entitlement data from multiple sources to a single identity
- Schedule both manager and application-owner certifications based on business priorities and monitor to ensure that reviews are completed on schedule
- Track revocations of or modifications to access and ensure that the appropriate changes are made throughout the IT infrastructure
- Generate reports to alert administrators to existing or potential access policy violations, remediations, and exceptions, and to demonstrate compliance with regulatory requirements

Minimal customization and programming requirements

As an enterprise extends its reach to include increasing numbers of external partners and their resources, it becomes increasingly important for the access certification solution to work seamlessly with those partners and their systems, applications, and data. It should not require substantial customization or programmatic development to work with external resources.

Integration with provisioning and role management

An access certification solution that can be integrated with a company's provisioning and role management processes enables complete life-cycle management of security policy violations and the access revocations that are associated with those violations. This closed-loop approach makes it possible to:

- Efficiently and effectively automate the removal of inappropriate access while capturing the appropriate audit information
- Increase compliance effectiveness by ensuring that business roles are consistently being defined based on correctly assigned access
- Get to the point where you are able to assign, attest, and audit access using roles

Depth of vendor expertise

The right access certification solution should come from a vendor with a deep understanding of the interrelationships between core identity challenges, processes, and solutions. The vendor should:

- Provide expertise in compliance management that encompasses expertise in inextricably related areas such as provisioning, role management, and directory services
- Demonstrate an understanding of, and the ability to effectively respond to challenges in areas such as Web access management and secure Web services
- Have the experience, expertise, and services to serve as a strong architecture and design resource that can guide your efforts to build an effective identity infrastructure

Chapter 4

Sun Identity Compliance Manager

Sun Identity Compliance Manager is a comprehensive solution for automating every aspect of the access certification process. It is specifically designed to be easily integrated with existing and planned components of the enterprise identity infrastructure.

Comprehensive capabilities

Identity Compliance Manager serves as a platform for automating the full range of existing manual compliance processes relating to access certification and access policy enforcement. The solution includes capabilities to:

- Automatically collect and correlate identity data from multiple enterprise resources
- Dynamically generate certification populations to ensure that certifications are performed by the appropriate business owners
- Automate detection of existing and potential policy violations in critical compliance areas such as segregation of duties (SoD) and unauthorized aggregation of privilege
- Report extensively on certification status, policy violations, and other access-related information, reducing the need to manually gather this type of data for audits

Easily integrated with existing infrastructures

Identity Compliance Manager leverages both agentless connectors and a general-purpose extract, transform, and load (ETL) based data collection capability for correlating entitlement data generated from any enterprise resource. This can dramatically:

- Reduce the time, cost, and complexity of implementing the solution
- Simplify the process of working with growing numbers of external partners and their applications
- Accelerate business value, with ROI typically achieved within 90 days of implementation

Part of a complete portfolio of identity solutions

Identity Compliance Manager is part of Sun's complete identity management portfolio for ensuring security and maintaining compliance, which means that it can:

- Integrate seamlessly with Sun™ Identity Manager for provisioning and auditing, Sun OpenSSO Enterprise for access management, Sun™ Role Manager for role management, and Sun™ Directory Server Enterprise Edition for directory services
- Identity Compliance Manager is also designed to integrate seamlessly with other identity access management products and with leading SIEM and IT GRC vendors to provide a comprehensive compliance solution.

From the recognized leader in identity management

Sun identity management has been recognized as a leader in a number of analyst reports, including the Gartner User Provisioning Magic Quadrant, the Gartner Magic Quadrant for Web Access Management, and the Forrester Wave report on provisioning.

Sun:

- Offers expertise not just in access certification in particular and compliance management in general, but also in provisioning, role management, and directory services
- Provides a complete portfolio of solutions to address emerging challenges in Web access management and secure Web services
- Goes beyond the technology to provide consulting services and support from a proactive services and enablement team
- Teams with business consulting and systems integration firms to help deliver additional consulting services for successful technology deployments

Product details are available at sun.com/identitycompliancemanager

Chapter 5

Identity Compliance Manager at Work in the Real World

The financial industry is undoubtedly one of the most highly regulated in the world, subject not only to broadly applied regulations such as Sarbanes-Oxley, but also to a growing number of industry-specific regulations. Accurately certifying user access — particularly with regard to high-risk transactions — is an important part of complying with the various laws that govern the industry. To improve its regulatory compliance, a leading global investment bank recently automated its access certification process using Sun technology.

Goal: Improve access certification

With 350,000 users distributed across 40,000+ business units, and with more than 100,000 accounts having access to high-risk transactions, the company required an effective solution for certifying access on a very large scale. The Sun solution made it possible to automate the entire access certification process through an implementation that included:

- Building an identity warehouse to serve as a common repository for application security data and user entitlement data for 350,000 users, along with business descriptions for entitlements
- Ensuring that SoD policies are defined and enforced across all users and applications, with 200+ SoD policies defined and applied to the 350,000 users
- Generating 10,000+ certifications (for 100,000 user accounts) and routing them to 15,000 business unit managers — all within a 60-day timeframe
- Performing a mass clean-up of orphaned accounts that were identified during the data-loading phase, which involved remediating 200,000 financially critical transactions across various applications
- Identifying SoD policy violations in 60,000+ user accounts and routing them to the appropriate business owners to revoke the errant access

Deployment of the Sun solution enabled the organization to achieve the following benefits:

- Reducing the amount of time and budget devoted to access certification by automating its traditional manual process
- Reducing the security and compliance risk associated with access to high-risk transactions
- Ensuring compliance with SoD policy by automating its enforcement across the enterprise
- Lessening the risk of being cited for noncompliance by accelerating the time required to certify access in general and to identify and remediate violations in particular

Chapter 6

Conclusion

Access certification technology is an invaluable tool for helping an enterprise manage its efforts to comply with the many regulations that govern businesses across a variety of industries today. Automating the certification process, increases certification accuracy and effectiveness, which in turn improves compliance and reduces risk. An Identity Compliance solution provides the organization with a clear understanding of their users' identities and access rights to critical business information and services and establishes compliance controls for ensuring that access is correct and remains correct. It enables the organization to answer those key questions:

Who has access to what, when?

Who approved those access privileges?

Are the access rights in line with policy?

With an automated solution, compliance requirements can be met and proven with minimum cost to the organization. Additionally, cost savings can be extended across the enterprise by utilizing the information gathered in a compliance exercise to refine your identity and access management program. Access control compliance is an ideal first step towards strengthening the security of business services and information, and reducing risk by evolving your identity management practices.

