WHITE PAPER: ENTERPRISE SECURITY

Managing Access to Critical Data for Protection and Privacy

Comprehensive Access Management for Data Protection and Privacy

White Paper: Enterprise Security

Managing Access to Critical Data for Protection and Privacy

Contents

Executive summary 4

The data defense imperative 5

Securing data and managing access 5

Identity management and the challenge of complexity 6

Limits of identity management 6

Access management today 7

Provisioning and access inflation 8

Infrequent audits 8

Unforeseen threats 8

Operational focus 9

Planning the transition 9

Comprehensive access management 10

Integrated provisioning 10

Frequent audits 10

Monitoring 11

Comprehensive access management and identity management 11

Symantec solutions for comprehensive access management 11

Securing data 12

Securing access: Auditing 12

Securing access: Monitoring 13

Executive summary

Protecting intellectual property and confidential personal, financial, and business information is a business priority, and often a legal requirement. To secure their data and ensure that only authorized people have access to it, organizations use a variety of access management disciplines. Access management includes identity management solutions that control permissions for critical data stores by managing Access Control Lists (ACLs). But identity management solutions in isolation risk access inflation, workarounds, and coverage gaps.

Comprehensive access management deploys identity management within a framework that includes disciplines for data protection, integration with hiring and promotion, and especially monitoring. Monitoring augments access management with a second line of defense, protection against unanticipated threats, a source of feedback for the continuous improvement of access management practices, and an audit trail.

The transition to comprehensive access management disciplines starts with an inventory and classification of data and a definition of appropriate IT security controls, along with the creation of a risk model to establish priorities. Typically, this planning process identifies areas of inappropriate access despite restrictive access rules, along with poorly defined controls, inadequate monitoring, and no real metrics for program effectiveness. Once under way, comprehensive access management relies on tight integration with business processes and frequent audits to maintain alignment with policy. And it depends on monitoring to identify, prioritize, and respond to unauthorized access.

Symantec solutions meet the demands of comprehensive access management. Storage solutions from Symantec provide a data protection foundation for access management disciplines. Symantec™ Control Compliance Suite helps keep access control definitions aligned with organizational policies and performs data center audits down to the file level, identifying areas of risk and documenting compliance. Symantec Security Information Manager adds monitoring to the solution set, with the identification of unusual activity, the prioritization and categorization of security events, and other tools essential for a documented, repeatable response program. Symantec Security Information Manager reports and analysis, together with Symantec out-of-the-box content for remediation and risk mitigation, support a closed-loop comprehensive access management program that meets today's requirements and stands ready to adapt to tomorrow's emerging challenges.

The data defense imperative

Protection against loss and theft of data—including personal and financial information about customers and employees—has become a top business priority and compliance mandate. On top of immediate losses from intellectual property theft, fraud, security breaches, and mishandled media, businesses face a wave of legislation and litigation triggered by high-profile disclosures of personal information. New laws are on the way to supplement privacy regulations and standards from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), California Senate Bill (SB) 1386, and European Union Directive on Data Protection.

The regulations themselves add costs and risks. First-year regulatory compliance costs an estimated US$3 million for every US$1 billion in company sales[1]—a significant burden in any tight-margined, competitive industry. Nor does compliance guarantee protection—legally mandated disclosure of data loss or breach exposes even a compliant company to fines, litigation, and loss of trust among employees, investors, and customers.

Business executives know that loss of trust is their most significant cost when data assets are compromised. Revenue and profits hinge on customer confidence; competitiveness depends on the ability to hire and keep quality employees and protect intellectual property. And the share price and cost of capital depend on shareholder and bondholder evaluations of company management. All suffer in the wake of a breach of data security or privacy.

All these costs—direct, indirect, and regulatory—are on the rise. The professionalization of data theft has resulted in faster, more sophisticated attacks against higher value targets. In the past, companies could self-insure against risks to their data. But today's corporate governance regulations such as the Sarbanes-Oxley Act and industry benchmarks like the Payment Card Industry Data Security Standard have made data protection a board-level issue. Few boards can tolerate that degree of risk—especially when regulations make governance their personal responsibility.

Securing data and managing access

Data protection and privacy stem from two closely related sets of disciplines: data security (protection) and access control (privacy). Secure data cannot be reached by anyone without appropriate permissions. Controlled access means only the right people have those permissions.

[1] A.R.C. Morgan Research, 2005

But when restrictions are too tight, they deny legitimate access to information, encouraging dangerous workarounds and slowing down every business process that depends on the protected information. Business information must remain secure, but it also must be available for legitimate use. Access management balances security and availability over the entire data life cycle, meeting the requirements of complex organizations as they change and grow.

Identity management and the challenge of complexity

Suppliers of applications, databases, and operating environments that hold critical data understand the need to balance data security and availability, so they build access controls into their products. But large data centers maintain multiple stores of data on platforms from multiple vendors, each with its own access control system. Managing access across these solutions has become a complex struggle.

To bring access management under central control and introduce some consistency and efficiency into the process, many large organizations are implementing identity management solutions. These solutions manage permissions for critical data stores, either directly or from an authoritative identity store. They promise easier employee access to required data sources, better data security, and documented compliance with data protection and privacy initiatives—all at reduced costs.

Identity management solutions may in fact eventually reduce the access management burden, but many organizations find them a challenge to implement:

- Their scale and complexity makes implementation time-consuming, politically challenging, and expensive.
- Access control coverage across multiple systems is still incomplete, encouraging workarounds and patchwork solutions.
- Upgrades and patches to underlying applications and databases can “break” identity management solutions.

Limits of identity management

Time and effort can overcome the practical problems of implementing identity management on a large scale, but more fundamental problems remain. Identity management is essential to comprehensive access management, but only as one part of a complete solution. A comprehensive approach must also include:

- Data protection, with disciplined processes for discovery, retention, and recovery
- Integration with relevant business processes such as hiring and promotion—the source of much of the business benefit from access management
- Monitoring, both as a second line of defense against threats that penetrate access controls and as a motivator for improvements in access management processes

Lacking these elements, most identity management solutions fail to deliver benefits on a scale commensurate with the investment of time and resources they require. Implementing data protection, process integration, and monitoring unlocks the identity management contribution to data and privacy protection and accelerates the efficiency and time-to-benefit of access management initiatives. Even organizations that choose not to implement a complete identity management solution—relying, for example, on staff to manage individual application, database, and file access controls—can realize significant returns from this approach.

To understand the advantages of a systematic, comprehensive approach to access management—with a full contribution from the identity management component—consider the following comparison with today's typical access control life cycle.

Access management today

Figure 1 shows a typical cycle of user access permissions at a large organization. New employees receive access to data they will need on or shortly after their hire date. New-hire business processes trigger some access provisioning. But new employees often discover other useful stores of data and gain access to them through a variety of formal and informal means.

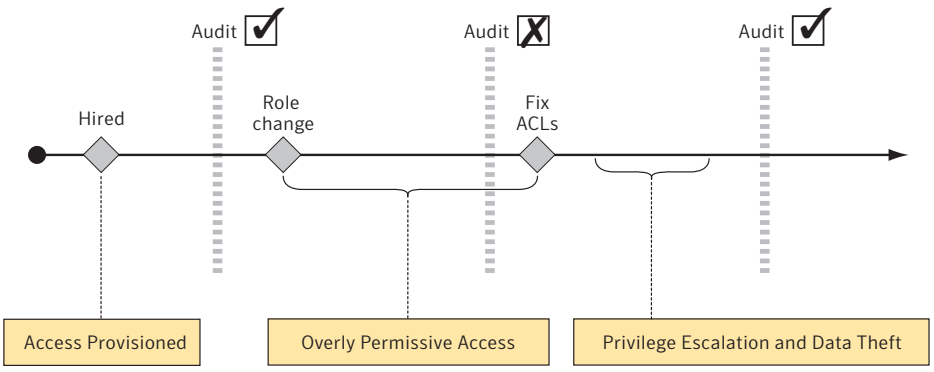

Figure 1. Typical user access cycle.

Provisioning and access inflation

Employees are more diligent about securing access to data they need than canceling access they no longer require. As a result, old permissions persist even as new ones are added, creating access inflation—permissions beyond those justified by employees' current business roles.

When employee roles change formally with promotion or reassignment, new permissions are added, but old ones often are not canceled, contributing to access inflation. In large organizations or those at which business roles change frequently, permissions may creep beyond policy limits.

Infrequent audits

Periodic audits are designed to correct access inflation. They realign access permissions with business responsibility by comparing ACLs for key data stores against the organization's policy. Audits catch policy exceptions and bring ACLs back into compliance. But auditing across multiple vendor systems is laborious, time-consuming, and often conflicts with high-priority scheduled IT activities or emergencies. As a result, audits tend to be infrequent, allowing permissions to exceed acceptable limits.

Unforeseen threats

Access controls for critical data are like door locks—essential, but insufficient by themselves. Organizations protect physical assets with locks backed by monitoring with cameras, motion detectors, and guards. Monitoring provides alerts and a second line of defense when locks are overcome or compromised by direct attack. It protects against threats that use unanticipated routes of access or methods of attack. And it creates the body of evidence needed for fair and effective response to security breaches, documenting who did what, when, and where.

Along the same line, electronic monitoring systems identify and alert operators to unauthorized access to critical data from accidental, internal, and external threats. Most solutions fulfill the basic need to identify and provide alerts to unusual activity. More sophisticated solutions provide a comprehensive response program and advanced reporting and analytics that help identify weaknesses in access control systems.

Access management approaches that lack monitoring place 100 percent of their confidence in the identity management and access control system. This allows thieves and adversaries to focus their attacks on a single point of vulnerability. Electronic and social attempts at privilege escalation, password theft, phishing attacks, and many other approaches are likely to exploit any such single point of failure successfully.

Operational focus

Today's access management environments are compromised by the habit of treating access as an operational problem for the IT help desk to address, rather than as a business process with roots in human resources, legal, risk management, and finance. Lacking tight integration with consistent business processes for employee hiring and promotion, project launch, vendor sign-up, and other key business events, access management remains reactive, informal, poorly defined, and ineffective.

Planning the transition

Organizations planning a comprehensive access management program—with or without an identity management solution—begin by analyzing the gaps in their current approach. Gap analysis covers at a minimum:

- Data inventory and classification, including the discovery of valuable information assets residing outside traditional security perimeters
- Identification of appropriate IT security controls to protect the data
- Definition of a risk model that incorporates asset value, cost and benefit of maintaining security, and residual risk

Most organizations see performance gaps in these areas:

- Inappropriate access to critical data, often despite onerous restrictions on access to the same data—clear signs of a broken process and a thriving workaround environment
- Poorly defined IT controls, designed for administrative speed under pressure and typically unconnected to any business process
- Inability to identify inappropriate access despite ACLs—signs of overcomplex processes and inadequate monitoring
- Inadequate monitoring of user activity and access, leaving no credible response mechanism in the event of inappropriate access

A comprehensive access management program does more than simply plug these gaps. It restructures access management around fundamental provisioning, auditing, and monitoring disciplines. This allows identity management solutions to provide a consistent defense against threats to data protection and privacy.

Comprehensive access management

Figure 2 shows the elements of a comprehensive access management program, with framework, process, and enabling technology organized to deliver data and privacy protection at defined levels, while reducing administrative burdens and costs. Although it resembles current access management structures, the differences are fundamental.

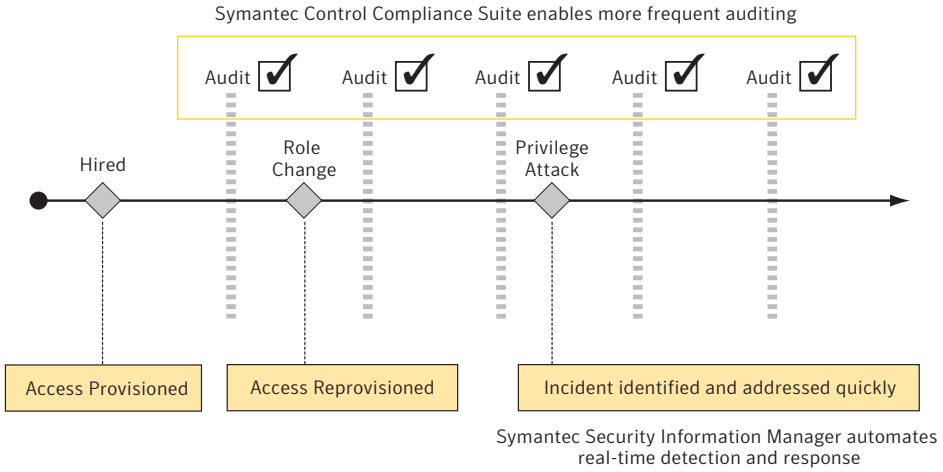

Figure 2. Comprehensive access management.

Integrated provisioning

Access provisioning, especially reprovisioning, is tightly integrated with the business processes supported, for example, hiring, promotion, and change of role. This minimizes the employee effort needed to secure the appropriate access, as well as the access inflation caused by permissions that outlive their business justification.

Frequent audits

Efficient, technology-supported audits run frequently, alerting administrators to provisioning or reprovisioning errors and out-of-date permissions so that access levels are aligned with organizational policy. This "lean" permissions environment reduces provisioning and audit workloads, even in organizations where roles and titles change frequently, improving efficiencies throughout the environment.

Audits also demonstrate compliance with access control policies, providing comprehensive reports on permissions and documentation of stakeholder sign-off.

Monitoring

The key value of comprehensive access management lies in its focus on monitoring. Monitoring helps organizations identify, prioritize, and respond to unauthorized access regardless of source, method, or intention. Equally important, it captures the information needed to analyze and correct deficiencies in the access management program itself. Unanticipated gaps in defenses can be identified, addressed, and corrected, placing access management on a continuous path of improvement.

Comprehensive access management and identity management

Within the framework of comprehensive access management, identity management solutions are easier to implement and administer and are more effective in safeguarding data and privacy:

- Provisioning disciplines enable centralized administration of identity management.
- Frequent audits simplify and reduce workloads for access administrators at central locations by keeping the lid on access inflation.
- Monitoring disciplines and technology—for example, automated, secure storage of logs—act as a backstop for identity management solutions, especially during the early stages of deployment before processes are stable.
- Feedback from monitoring closes the access management loop, supplying the information necessary for continuous improvement of identity management and other core processes.

Comprehensive access management frameworks help improve time-to-benefit and return on investment from identity management solutions and deliver the early gains that help cement management support and employee buy-in. Even in organizations not planning full-scale identity management programs, relatively nonintrusive access management improvements can deliver much of their benefit, at a fraction of the total cost.

Symantec solutions for comprehensive access management

Symantec solutions are available to establish or augment access management environments, approaching full comprehensive access management. From data protection to monitoring, the solutions provide advanced technology and process support for key comprehensive access management activities.

Securing data

Symantec storage solutions, including Symantec Enterprise Vault™ and Veritas NetBackup™, automate the processes for discovery, retention/destruction, archiving, backup, and recovery of critical information assets. The capabilities of these solutions are well documented, and they are excellent candidates for building the data protection foundation on which comprehensive access management relies.

Securing access: Auditing

Symantec Control Compliance Suite (see Figure 3) performs audits of IT controls in heterogeneous environments, including access controls and permissions. It provides:

- Access control definitions aligned with organizational policies, including definitions used with identity management solutions. Templates for and updates to important regulations and standards also make this product ideal as a planning aid for policy compliance programs.
- Environment scans that define the audit range across applications, databases, and operating systems accessed since the preceding audit, down to the individual file level. Administrators see a single, unified report of permissions across the entire data center.
- Rapid analysis of access and entitlement that quickly identifies policy exceptions and helps find "hot spots"—users, machines, or information assets with permission histories that may warrant closer investigation.
- Documentation that information owners and stakeholders have attested to the legitimacy of access, down to the individual file level.

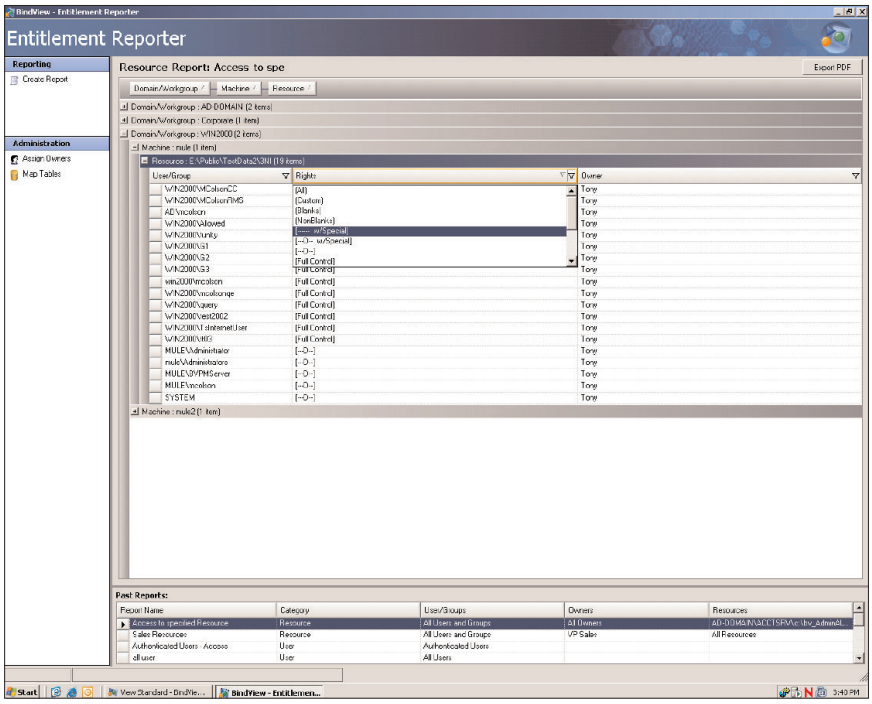

Figure 3. Symantec Control Compliance Suite reports current permissions for access to critical data and facilitates attestation from stakeholders.

Securing access: Monitoring

Symantec Security Information Manager (see Figure 4) is the monitoring component in Symantec's access management solution set. The solution supports:

- Identification of inappropriate or unusual user activity according to preset rules
- Prioritization and categorization of security events, speeding up analysis by moving important events to the top of a list offering a rich view into stores of critical data
- Documented and repeatable responses to events and patterns, from generation of work tickets through alerts to an administrator's mobile phone, to complete remediation and risk mitigation strategies from Symantec's leading Global Intelligence Network and response teams
- Analysis of event patterns for policy reviews and continuous improvement programs, with out-of-the-box reports and dashboards to identify common gaps in security and access controls and repetitive failures

Figure 4. Symantec Security Information Manager dashboards and reports help ensure that comprehensive access management programs meet their stated goals.

Symantec Security Information Manager automatically detects the full range of access violations, including privilege escalation, account and password guessing attacks, and null login (see Figure 5). Like the other solutions in the series, it works across Windows®, UNIX, and Linux® platforms, with SQL and Oracle® databases, and with Active Directory and RSA SecurID authentication platforms. Symantec Security Information Manager supports the monitoring requirements of comprehensive access management with:

- User activity tracking across products and platforms
- Event details including the who, what, when, where, and how of each access event
- Compliance tracking templates to identify violations across products and sources, including out-of-the-box reports supporting key regulations

- Scalable long-term storage of log and event information to support forensic or compliance queries
- Rich asset views to make sure threats to the most sensitive data are prioritized appropriately
- Out-of-the-box rules identifying suspect activity, customizable to unique customer requirements

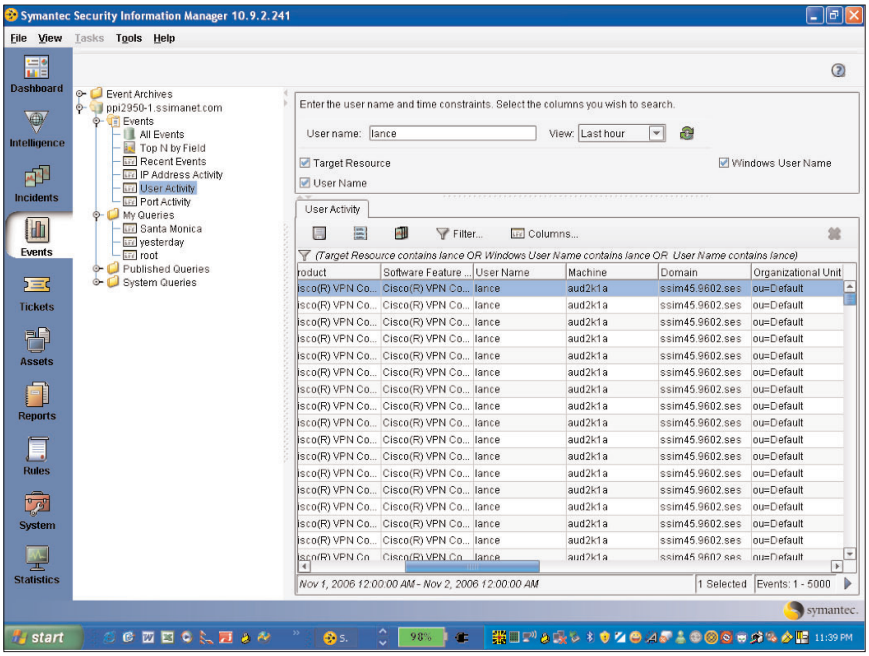

Figure 5. Symantec Security Information Manager records and provides alerts for all user activity on critical systems.

Symantec Control Compliance Suite audits deeply and often to keep access permissions in line with policy, as Symantec Security Information Manager automates real-time detection of and response to events that penetrate or avoid the access control perimeter. Combined with thoughtful, policy-based access control and identity management, these solutions enable IT to address the challenge of protecting information assets, helping to safeguard employee and customer privacy and documenting compliance with relevant regulations and standards.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, Enterprise Vault, NetBackup, and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
Printed in the USA. 12/06 10745925