Exploring Identity Management: Selecting Identity Management Tools

A White Paper Prepared for
IBM Tivoli Software
September 2003
Exploring Identity Management: Selecting Identity Management Tools

Table of Contents

Introduction ......................................................................................................................................................................... 1
The Challenges of Managing Identities .......................................................................................................................... 1
  Dealing with Change and Employee Mobility ................................................................................................................ 2
  The Need for Integration .............................................................................................................................................. 2
The Impact of Global Regulatory Requirements .............................................................................................................. 3
Identity Management and the Enterprise ........................................................................................................................... 3
  What is Identity Management? ...................................................................................................................................... 3
  Identity Management Life Cycle ................................................................................................................................... 4
Investigating Identity Management Solutions ................................................................................................................ 5
  Investigation Checklist .................................................................................................................................................... 5
  Selecting Products ........................................................................................................................................................ 6
Password Management ......................................................................................................................................................... 6
  Architectural Considerations .......................................................................................................................................... 7
Orphan Account Elimination .......................................................................................................................................... 8
  Automation Through Policy-based Management ............................................................................................................. 8
Process Workflow .............................................................................................................................................................. 9
  User Provisioning .......................................................................................................................................................... 9
Audit Trails ........................................................................................................................................................................... 9
Other Considerations ....................................................................................................................................................... 10
Conclusion ......................................................................................................................................................................... 10
Exploring Identity Management: Selecting Identity Management Tools

Introduction

The characteristics of today’s businesses are drastically different than they were even a decade ago. In the past, only certain business segments, like retail, conducted their business through wide-open doors—welcoming their customers as well as welcoming their vendors to come in and view their wares. Today, almost all businesses conduct their commerce through open doors—whether it is through a Web site, allowing business partners to access the company’s IT resources, or conducting business through a storefront. As Web services becomes more mainstream, that openness will significantly increase. It is clear that the doors of the enterprise are definitely wide open for business. While this openness provides business opportunities, it also presents security challenges and potential risks. In addition, internal users, such as employees, temporary workers and contractors have access to sensitive internal systems. The cost of managing access for the disparate groups of users is expensive, and the risks are increasing. It is because of this added cost and risk that identity management is an area of increasing attention and interest for enterprises.

It is no longer sufficient to just manage passwords. When trading partners, customers or employees are allowed broader access to the infrastructure, it is important to carefully identify who the user is, what they need access to, what they have access to, what they can do and what can be done with their information, all while ensuring compliance with corporate policies. Identity management goes way beyond simple password management, but what is it really? With vendors defining “identity management” in many different ways, it can be confusing. In order to dispel the confusion surrounding identity management, this paper will explore the issues of managing identities, provide a definition for the term and discuss what to look for in identity management tools.

The Challenges of Managing Identities

In the course of a typical day, an employee of a company may use ten different applications that are running on more than three different operating system platforms. Each of these systems and applications typically has security profiles that must be added, changed, or deleted manually. This same employee also performs duties in several different roles (for example: employee, line of business manager, chairman of the committee for a strategic company initiative, and liaison to a trading partner), with each role requiring job-specific access to different corporate resources in order to do the job. For each of these roles, the employee must be granted access to only the information that he needs for each of his job roles.

Exacerbating the problem is the fact that each application and system may have its own security, each with its own password and authorizations, that are separate and discreet. In addition, the identity, access, and authorization data for an employee may be scattered across the corporate infrastructure in a multitude of sources, from a human resources (HR) database, to disparate application security databases. Multiply this scenario by tens of thousands of employees, customers, and business partners who have some type of access to the corporate infrastructure. It then becomes clear that the task of managing the seemingly infinite views of the many resources that need to be protected, the multitude of users, and the gigabytes of data stored in several security databases, is expensive, and potentially fraught with inefficiencies and risks. This complex, fragmented, and dispersed environment, if not managed correctly, may expose the enterprise to unnecessary risk by allowing access to corporate assets unknowingly. And when it comes to security, ignorance is certainly not bliss.
Dealing with Change and Employee Mobility

The dynamic nature of the business environment adds another dimension of complexity to managing identities—change is on-going, and the access rights must be updated quickly to reflect the new realities. For example, hundreds or thousands of employees may be simultaneously terminated as the result of downsizing, employees are promoted and transferred to other departments, the job duties of employees may change due to business changes, and new employees are hired. The existence of orphaned accounts, which are accounts that cannot be associated with current authorized users, opens an opportunity for unauthorized access. Changes, both planned and unplanned, must be handled quickly and efficiently to effectively minimize the risk of unauthorized internal and external access to corporate assets. The lag time must be reduced between the actual change and when the change is reflected in the access rights, and the current changes must be reflected comprehensively across the infrastructure. When users have various accounts that are scattered across the enterprise, without a central system of record for all accounts, it is virtually impossible to be effective or efficient using manual methods to comprehensively change or delete all accounts associated with that employee. With so much employee change going on and the many interactions between employee and data, it is too easy to miss making necessary security changes, thus increasing the risk to corporate resources.

Employee mobility presents a challenge for managing identities. Changing jobs and job duties within the enterprise introduces one type of employee mobility; another example is business travel. As employees travel and use corporate resources, managing access is only one aspect to consider. It is just as important to ensure that employees are in compliance with corporate policies when accessing information from outside the corporate borders. For example, if corporate policies prohibit employees from downloading customer information in clear text, then those policies must be enforced by access policies. Compliance presents another challenge.

The Need for Integration

Managing identities and access control must be done in an integrated manner, in order to protect the integrity of the enterprise. Integration is the key to effectively managing identity and access. Without it, the company is leaving itself open to a high degree of risk. Here is an example of the risks that might be involved. The HR database may have been updated to reflect a terminated employee. But if identity and access are not coordinated effectively across the enterprise’s infrastructure, the appropriate changes may be made to some but not all of the security systems that relate to that employee. The terminated employee may still have access to the corporate Intranet, the company’s business partner extranet, customer contact information, or sensitive company information. Just imagine the risks involved and the company’s exposure if this employee goes to work for the company’s competitor with unauthorized access to the company’s information at his fingertips. Multiply this problem by all of the employees that leave the company in a year, and it opens up the potential for huge security and business vulnerabilities. This example clearly shows why enterprises need an integrated identity management approach. The lack of integration between security tools and/or security databases can introduce vulnerabilities that are unintentional yet potentially damaging to the enterprise.

As enterprises continue to open the gates to their infrastructures to facilitate collaboration with business partners, and allow external access by employees via the Web, identity management becomes increasingly important. When enterprises adopt Web services in the mainstream, and application infrastructures become more loosely coupled, identity management will be a necessity. In a Web services world, the resources are even more widely dispersed than they are today. One part of an application may be serviced in-house, but external service providers doing credit checks may complete several other components. In such a loosely coupled environment, access control and identity management are essential.
The Impact of Global Regulatory Requirements

Governments around the world are beginning to regulate the privacy and security of information. Examples of these regulations include the Health Insurance Portability and Accountability Act (HIPAA), the European Union Data Protection Directive, and the Gramm-Leach-Bliley Act. These regulations dictate how specific personal information is used, as well as requiring the organizations that handle the data to keep it secure and private.

Compliance with governmental regulations related to information security and privacy are requirements that carry penalties for organizations that do not comply. Companies affected by these regulatory requirements must develop security processes that protect the data from disclosure, and the ability to prove that they did what was necessary to protect the data, in the event that they are accused of non-compliance.

Identity Management and the Enterprise

There is confusion in the market about the definition of Identity Management. This is partly due to the fact that vendors conveniently define Identity Management according to what their products can do. However, in order to truly reap the value that Identity Management offers to enterprises, a broader, comprehensive definition of Identity Management is a must.

What is Identity Management?

Identity Management is a comprehensive, process-oriented and policy-oriented security approach that:

- **Establishes and manages the identity of the user throughout the life cycle of that identity.** This begins from the initial provisioning of the user’s identity; including the defining of access rights and following a logical work flow to complete the provisioning process. During the life of the identity, it will be modified to reflect any actual changes that affect the identity definition, such as changing departments, and altered duties. Then at the end of the life cycle, removing the identity of an employee who is no longer working for the company.

- **Uses policies to define access rules to resources that the user requires in order to do their jobs and fulfill their roles.** Using policy to manage identities by groups and roles provides consistent and automated updating of identities as users move between departments and jobs within the organization.

- **Defines what the user can do with resources.** Is the user allowed to update the data, only view the data, or create data?

- **Facilitates the processes for access approval, user provisioning, and compliance reporting, as well as other identity management processes.** Processes are extremely important for managing identities—processes for approvals must be followed to ensure that the access rights are appropriate for the employee in question. When provisioning the user, there is a logical flow and a sequence of steps that must be followed in order to properly provision the user. Those processes must also tie into non-IT segments of the workflow. For example, periodically validating that business partner personnel and contractors are still valid and authorized users. This ensures the security of these accounts by eliminating the accounts of contractors or business partner employees who no longer work for the company, or changing the access rights for anyone whose responsibilities have changed.

- **Enforces access control across the extended enterprise.** Leveraging the user identity information and combining it with defined policies to enforce user access in a consistent and comprehensive manner across the extended enterprise. The access rights for the user is enforced by policy, and is based on
specific attributes in the identity data, such as the department they are assigned to, title, location and more. This centralized approach avoids the need for explicit access definitions that are applied haphazardly on different devices and difficult to manage.

The granularity of access control should also extend to controlling subsets of access. For example, a customer service representative may require access to customer information but not all customer information, so they are limited to seeing just the customers’ name, address and phone number.

- Manages information privacy that complies with regulatory or corporate requirements. Having the ability to specifically identify the information that must be kept private, and guarding that privacy.
- Ensures security compliance with corporate policies. Policy-based management imposes and enforces corporate policies upon the management of the identities and access rights.
- Performs these functions in an integrated, automated manner. Policy-based management allows the identities to be managed automatically using access rules. As users fit the qualifications for the rules, then the rules are automatically applied to their identities.
- Integrates with directories and other data stores. Directories hold a wealth of identity related information. It would be inefficient to duplicate the information that is already stored in the directory, so leveraging that information by pulling from that data, as needed, makes a lot of sense.
- Consolidates and integrates identity information. Leverages identity information that already exists.

As can be seen above, Identity Management goes far beyond password management. It takes a life cycle approach to the management of an identity and access control from its creation, managing the changes that occur during its lifetime, and then finally removing the identity when the user is no longer an active participant. It holistically manages the notion of identities by leveraging existing identity information by integrating with directories that store identity information. It also has the ability to integrate with HR systems to access any identity information on an employee, such as hirings, firings, promotions, and transfers. It also touches on privacy issues that are closely tied to the identity of the user.

By taking this broader approach to managing identities and the resources closely connected with identities, it minimizes the risk for enterprises because the processes are dealt with using a holistic approach, not a fragmented one. The identity is managed through all of the stages of the processes to ensure consistent, handling of the identity.

Identity Management Life Cycle

Identity management manages the life cycle of a user’s identity. Figure 1 depicts the identity management lifecycle and how the facets of identity management described below fit into the lifecycle.

- User Provisioning: The identity management lifecycle begins with the provisioning of the user.
- User Management: Once the user is provisioned, the next phase of identity management is the ongoing maintenance of the users’ access rights, passwords, and accounts. Applying policy-based management to the user’s identity can assist in automating the management of access control. For example, policies can be set up that define the resources, applications and functions that a user in the accounting department should have access to. So if an employee is transferred into the accounting department, they are automatically granted the access rights ascribed to their department.
- Policy Management: Policy-based management is the glue that pulls all of this together. It allows automatic updating of access rights, based on membership in a particular group or department. In
addition, it also ensures that corporate policies are enforced consistently across the enterprise. Policy also allows facile management of large numbers of user accounts, providing scalability of the solution.

- **Privacy:** In response to privacy regulations, enterprises must secure the privacy of certain types of information that are related to specific individuals. The privacy regulations usually define the subset of information protected by the regulations.

- **Account Closure:** Deleting the account when the identity is no longer needed.

**Investigating Identity Management Solutions**

When considering identity management solutions, it is best to develop a strategic approach to managing identities. Be sure to understand the identity management solution's ability to integrate with other products that provide additional identity management functionality. And of course, it should fit into your strategic plan. You may elect to deploy user provisioning first, because it meets a major point of pain for your company. Then later deploying other parts of an identity management strategy. However, before purchasing the product, be sure that it is a strategic choice and not just a tactical, low cost choice that happens to solve an immediate problem. The strategic choice fits in with your identity management strategy, and there is an additional advantage if it can be deployed like building blocks, a piece at a time. But in the end, the strategic choice does eventually equal a whole; the tactical choice does not.

**Investigation Checklist**

Here is a quick checklist to use when selecting a solution:

- Understanding the business needs of your company.
- Are there specific requirements of identity management that are required for near term and long term business initiatives?
- Do privacy regulations apply?
- Are there special customer-related or partner-related issues that must be considered?
- What are the economic drivers, such as reducing operations costs, administrative costs, and help desk costs, that are driving the need for identity management?
Exploring Identity Management: Selecting Identity Management Tools

- Determine your corporate security needs
  - What are the data security requirements for my company – very granular or broader?
  - What are the user security requirements for my company – are they typically assigned by role, department, or both?
  - Are there existing vulnerabilities or risks that need to be mitigated?
- Develop security policies
  - The security policies lay the groundwork for identity management, that is part of the broader security strategy for the company.
  - Also develop the processes that will communicate the security policies to employees and enforce them.
- Defining security strategy/architecture
  - Design your security strategy, and the architecture that will allow your company to realize the benefits and reduced risk. The architecture that you develop will ultimately affect the types of solutions that you will select.
  - Apply the right solution to solve the problem. There are many different approaches to solve your organization’s problems. The trick is selecting the right ones. For example, agentless management technologies are quick to deploy and easier to maintain, but a price is paid in a reduced level of security. Agent-based management technologies take more time to deploy the agents, but they offer a richer set of management capabilities, such as encryption and anti-spoofing capabilities. Agents also enforce policies by preventing anyone from changing entitlements without going through the proscribed processes.
  - Does the solution fit in with security strategy and architecture?
  - Is the solution integrated across the enterprise? An integrated solution provides more of an end-to-end approach.
  - Evaluate and select the identity management products

Selecting Products

Evaluating and selecting products can be challenging—not all identity management solutions are alike. Some vendors create confusion when they label their solution as identity management solutions, even if they are only performing a subset of functionality. For example, the solution may only do user provisioning, but the vendor claims that they are an identity management solution. So buyers beware... Arm yourselves by educating yourself on what a comprehensive identity management solution should contain (which is the intent of this paper) and then use that definition to measure the solutions that you are evaluating. It involves digging through the marketing literature provided by vendors, as well as relying on intelligence from other sources to find out what the product actually does. Once the research is gathered, it becomes a matter of sorting out the product offerings to see which ones fit in with your security strategy, architecture and security policies. Finally, ending with picking your top choices.

Password Management

Managing passwords is a potentially time consuming task. Look for productivity features, such as self-service capabilities, where the user can find a forgotten password independently. Lost passwords are a major
cause of additional calls to the call center. By providing self-service capabilities where users can independently determine what their passwords are without calling the help desk, can save users and help desks both time and money. Users can also use the self-service feature to change their passwords as required by company policy.

The administration of passwords should be easy to manage, and designed with automated capabilities that leverages your IT staff by not requiring them to manage each identity individually. Password management is one component of access control. Policies can also assist in the administration of passwords, where the user is only allowed to reset their password with valid passwords that conform to corporate policies.

Most users are asked to remember quite a few passwords – a password to sign into their financial application, another one to log into the corporate Intranet, and yet another to log onto the corporate extranet, still another to access the Internet, yet another to access email, and one more to sign in to a collaboration portal. When faced with memorizing too many passwords, users resort to having the passwords stuck on their monitors using sticky notes, or selecting easy to remember (and easy to guess) passwords. Single sign-on allows a user to sign on once and the single sign-on product authenticates the password and user ID to each application and system.

**Architectural Considerations**

From an architectural standpoint, it is important to understand the different approaches that the products take to address identity management – so that in the end, the product that you purchase is exactly what you thought it was. With identity management, vendors can take one of two approaches with variations in between. The first is an application-oriented approach, and the second is the infrastructure-oriented approach.

The application-oriented approach is a point solution that focuses on solving a specific problem. It is sometimes used to provide a quick fix to a problem, at a low cost, and it offers “good enough”, stop gap capabilities. As a stand-alone product, there are usually minimal installation and integration interdependencies.

By contrast, the infrastructure-oriented approach is a product suite solution that is designed to address the broader issues of security across the enterprise. It offers a tight integration with adjacent security systems and provides more comprehensive capabilities. Because it is a broader solution, it is more adaptable to a wider range of processes and needs in the security environment. In addition, its integration with other systems offers a cohesive solution that can grow with the needs of the enterprise as it grows. Along with growth, the product must be scalable to handle the larger volumes of the enterprise.

When comparing solutions, be careful to compare apples to apples and know what you are really getting. The application-oriented solution will invariably have the short-term advantages of quick deployment and lower cost. However, in the long-term, these solutions may not scale with the strategic needs of the company. The infrastructure-oriented solution usually requires more work up front, but keep in mind that the issues here are not typically product related; they are organizational. For example, what policies should be applied to the accounting department? Or what resources should a mid-level sales manager have access to? Although sorting out these issues is not initially an easy thing to do, from a strategic view, it is the right approach.

When evaluating identity management solutions, be sure to understand their ability to integrate with other products that provide other identity management functionality. You may elect to deploy user provisioning first, because it meets a major point of pain for your company. However, before purchasing the product, be sure that it is a strategic choice and not just a tactical choice. The strategic choice fits in with your identity management and overall security strategy, even though it can be deployed like building blocks, a piece at a time. But in the end, the strategic choice does eventually equal a whole; the tactical choice does not.
Integration is an important aspect of the architecture that must be considered at several different levels. First, there is integration with the other products in a product suite, and interoperability with other security management products. If you like one component of the product suite but you also like another vendor’s complementary product, “Will these products work together out of the box?” And are the products integrated across the enterprise to provide a comprehensive approach.

Identity management solutions should have a central, authoritative database for user information that is automatically synchronized with existing identity information stored in places like corporate directories, HR databases, business partner lists and more. A central database is necessary because other sources of identity information are very focused and are not typically complete—for example, HR only contains employee information, and not contractor or business partner user information. A central, synchronized store of identity data ensures up-to-date and accurate identity information. An identity management solution must play an active role in maintaining the accuracy of the identity information – it is essential for effective management. An identity management solution that does not assume this responsibility is basically relying on manual methods for updating identity information, and should be avoided because it cannot offer effective identity management.

The identity management solution should also have the capability to integrate with non-IT systems, such as HR systems, which offer a more complete approach to managing identities by tying into the definitive source of employee information.

The products should be flexible enough to allow your company to do what it needs to do. Today’s business environment changes so rapidly and the change is constant, so the flexibility of the solution to adapt to business driven changes should not be overlooked. If the product is not flexible, look for a product that is.

Orphan Account Elimination

A major exposure of security is the existence of accounts that do not belong to a currently valid user. As employees leave the company or move to other locations, there may be cases where, an account was not deleted, which creates orphaned accounts. If orphaned accounts are not regularly reconciled and eliminated, you are allowing an access point for ex-employees to continue accessing your data and resources.

Integration with other identity data sources is an important factor for detecting orphaned accounts. For example, tapping into the HR database will show that Joe Smith was terminated two weeks ago, but that he still has an account on a departmental system. Identity management solutions that do not integrate with other systems cannot effectively eliminate orphaned accounts. What do you do if the user cannot be found in an existing authoritative system? It is here that the identity management system needs to “fill in the blanks”. Since Joe is no longer an employee, based on policy, the account should be eliminated.

Automation Through Policy-based Management

An identity management solution should employ policy-based management to simplify the administration of identities by supporting role-based access rights. As employees are promoted, hired or moved to new job duties, changing their access rights to reflect their new roles happens fluidly and automatically because the access rights are tied to the roles, rather than being “hard-wired” to the user.

Access control can be more automated, if it is defined by groups that an employee belongs to, such as a department or division. Policies facilitate the granting of access to resources and applications that employees require to do their jobs, and that are relevant to their jobs.
Policy-based management can also control updates to user information. Only authorized personnel are allowed to make changes, and they must also have the authority to alter the information that they want changed. Policy also has a role in ensuring that the changes conform to corporate policies. For example, when users change their passwords using self-registration features, the policy compels them to select passwords that conform to corporate password conventions.

Finally, policy-based identity management should also provide the capability to ensure compliance with corporate security policies and governmental regulations. The ability to manage data privacy in today’s climate of increasing governmental scrutiny is becoming a necessity.

**Process Workflow**

The task of managing identities is very dependent upon processes, such as approval processes to grant access to resources, and processes for provisioning users. It stands to reason that an Identity Management solution should include and facilitate the management of process workflows.

In some cases, the most difficult part of implementing a comprehensive Identity Management solution is defining the business processes and policies that are needed to effectively manage user identities. These are typically organizational issues, not product issues, that require work initially. But once they are established, and policies are established, managing identities becomes much simpler to deal with. Process workflow capabilities helps to make this process easier to establish.

The processes may span to non-IT systems and processes, and the solution should have the capability to integrate and work with other systems.

**User Provisioning**

User Provisioning follows a process that is different in each organization. So, the provisioning solution should have work flow capabilities that can be modified to model the work flow for the company. This includes the initial setting up the user account, which could be triggered from an integration with the enterprise’s HR system. In addition to setting up the user into groups or roles, the solution should also facilitate the approval processes.

The user should be provisioned quickly and efficiently, so that they have rapid access to the applications and resources to do their jobs. Any delays may hamper their assimilation into the company. So the approval process must be flexible enough to keep on top of requests that are just sitting on the “desktop” of a supervisor.

The User Provisioning process should also be flexible enough to tie into non-IT tasks, such as requesting the installation of a phone and computer for the user. Having the ability to include all tasks in the work flow of provisioning a user ensures that all of the tasks are consistently completed for each new employee.

**Audit Trails**

Audit trails are an absolute necessity for security. Having the ability to review all of the adds, changes and deletions related to access rights and account administration is an important step in securing the enterprise. Time stamped entries help to piece together the sequence of events. Each entry must include information about the approval or denial of any changes, who changed it, and the actions that were executed.

Logging the data is necessary for auditing, however, reporting and analysis of the audit information is the most important component of auditing the security processes. Good reporting can help to clearly see when processes are bypassed, to help spot unusual activity, or to do normal activity reviews. With the large amount
of data that is collected for auditing purposes, effectively synthesizing the information into a usable form is essential. This includes being able to run on-demand reports by user, managed resource, selected time ranges, administrators and more.

As regulatory and audit requirements escalate in priority, audit trails are essential to managing compliance with the regulations, as well as being a useful tool in proving company compliance. The consequences for non-compliance can cost the company time and money, in dealing with legal issues and penalties that may be levied against the company. In addition, maintaining customer trust and confidence in how your company secures their personal information and your internal infrastructures is even more important.

Other Considerations

Another consideration is which approach will you take – point product, product suite or a hybrid solution that combines both kinds of products. The answer depends on the needs of your company, your objectives for this solution, how it fits in with your corporate security strategy, and existing products that you already are using. There is no right answer for every situation. But what you do want to investigate is the interoperability of the products that you ultimately select. Whether it is a point product or a component of a product suite, they should be interoperable with other security products from other vendors.

Conclusion

Identity Management systems are not all alike. But now that you are armed with knowledge of the capabilities that a comprehensive Identity Management system should have, the task of evaluating and measuring the available solutions should be much easier.

When selecting any kind of product, be sure to think strategically and take the bigger picture view of what you are trying to accomplish. It protects the investment that you are making, when it fits into the broader strategy of the company. And it also ensures that the effort that is expended will pay back in benefits for the long term.

Identity Management solutions are not alike, but companies are not alike either. The challenge is to select the right solution for you and your company, and to well position your company to effectively manage its identities in the future.
About Enterprise Management Associates, Inc.

Enterprise Management Associates, Inc. is the fastest growing analyst firm focused on the management software and services market. EMA brings strategic insights to both vendors and IT professionals seeking to leverage areas of growth across e-business, network, systems and application management. Enterprise Management’s vision and insights draw from its ongoing research and the perspectives of an experienced team with diverse, real-world backgrounds in the IT, service provider, ISV and publishing communities.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc.

All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

© 2003 Enterprise Management Associates, Inc. All Rights Reserved.