



Business Strategy Report Identity and Access Management Industry Overview

Business Strategy Report

June 25, 2005

Business Strategy Report / Business Strategy Report Identity and Access Management Industry Overview

Printed in the United States of America.

Copyright © 2005 Edison Group, Inc. New York. Edison Group offers no warranty either expressed or implied on the information contained herein and shall be held harmless for errors resulting from its use. Business Strategy Report is distributing this document and offers no warranty either expressed or implied on the information contained herein and shall be held harmless for errors resulting from its use.

All products are trademarks of their respective owners.

First Publication:

June 2005

Produced by:

Edison Group, Inc. Security Ana

Table of Contents

Introduction.....	1
IDENTITY MANAGEMENT.....	1
ACCESS MANAGEMENT.....	2
BUSINESS CHALLENGES.....	4
BENEFITS OF IAM SOLUTIONS.....	5
LEGAL BENEFITS.....	5
ADMINISTRATIVE BENEFITS.....	6
SOFTWARE DEVELOPMENT BENEFITS.....	7
SECURITY BENEFITS.....	8
FINANCIAL BENEFITS.....	9
MARKET REQUIREMENTS FOR IAM SOLUTIONS.....	9
IDENTITY SOLUTION DESIGNED AROUND BUSINESS POLICIES.....	9
STRONG AUTHENTICATION.....	10
FEDERATED IDENTITY MANAGEMENT.....	10
EASE OF IMPLEMENTATION.....	10
DATA SECURITY.....	11
RESILIENCY.....	11
MANAGEABILITY.....	12
REPORTING TOOLS.....	12
SUPPORT OF STANDARDS.....	13
TOOLS AND UTILITIES.....	13
COMPLETENESS OF THE SOLUTIONS.....	13
OVERVIEW OF THE MARKET PLAYERS.....	14
IBM/TIVOLI.....	14
SUN/WAVESET.....	15
CA/NETEGRITY.....	15
NOVELL.....	15
HP.....	16
MICROSOFT.....	16
ORACLE/OBLIX.....	16
Summary.....	16

Introduction

Recent advances in distributed business computing have enabled a wide variety of LAN- and Internet-based means of accessing business data. Such technology (including off-the-self and custom-grown applications) must offer appropriate data security, differentiated access privileges, and transaction auditing systems. Since operating environments and application packages often have their own authentication and authorization systems, achieving uniformity would call for a separate security layer that would handle all the underlying systems and act as a repository of all authentication and authorization data. This security layer would ultimately be responsible for synchronizing data across multiple directories, handling authentication and authorization requests for the applications, storing the authentication and authorization data for the entire corporation, and offering adequate management for an auditing functionality. Such features are offered by modern Identity and Access Management (IAM) solutions. IAM projects are usually more complex than the majority of IT initiatives, due to the number and diversity of identity stores, protocols, encryption mechanisms, policies, and governing bodies that must interoperate. The present paper will address the access and identity challenges facing large and midsize companies, possible IAM solutions and the benefits of such solutions. We will also overview the major components of an IAM offering and briefly describe the most prominent IAM players.

Identity Management

Identity management can be defined as processes and technologies designed to provide centralized capabilities for managing the entity identity lifecycle (creation, modification, self-service, synchronization, reporting, and revoking). Identity management solutions address the following aspects:

- Provisioning of user identity
- Centralized management capabilities
- Federated identity management
- Consolidation of identity information

Provisioning provides the automated capability for the creation, modification and deletion of user accounts across multiple systems. Such management operations can be performed manually, automatically, or scripted to be executed as a response to a particular application event, such as user suspension in the Human Resources application.

Centralized user management provides the underlying automation for updating user profile information in business applications, such as translating personal and contact information from HR applications to messaging systems, employee directories and custom applications. The user management paradigm includes functionalities such as fine-grained

delegated administration, approval workflow, and user self-service. The presence of full-fledged workflow and self-service interface streamline user management operations since it simplifies the approval process for the new accounts and eliminates helpdesk calls related to password or account resets.

Federated identity management describes the technology to securely share trusted identities across the infrastructure of different business entities such as service providers, partners, etc. The technology simplifies the affiliate services and business partnership by allowing users to be identified to all the systems, networks, and web portals they have the right to access with a single logon.

Consolidation of identity information can be implemented either thru the centralized data store or via directory brokers. A centralized data store (meta-directory or directory-vault) is the master data repository acting as the primary source of authentication information. An underlying technological framework enforces two-way synchronization between the directory vault and the directories of the linked business applications and network services. The framework is responsible for ensuring that the password policies are compatible across the managed systems and for enforcing these policies bi-directionally. Bi-directional data synchronization is required if password changes are to be initiated from the managed system.

A directory broker-based solution takes a different approach to managing credentials. A collection of connectors is responsible for converting credentials on-the-fly during a cross-directory exchange of authentication data without relying on a single directory store. Both approaches have advantages and disadvantages. Whereas the meta directory-based approach requires application and OS plug-ins – thus being more intrusive – it offers tighter integration with the managed platform and, by being platform specific, allows for better error checking and more built-in logic in data processing. Several vendors – primarily as a result of mergers and acquisitions – offer both solutions simultaneously.

Access Management

Access management is defined as processes and technologies designed to provide centralized capabilities for managing the access to a given application or operating environment with high granularity of access, adequate logging, group membership, ability to implement dynamic access rules, support of external rule storage and ability to perform step-up and chained authentication when accessing information that requires higher level of privilege. Such access can be implemented in intrusive form, in which a piece of code is embedded as a plug-in into the managed Web or application server, or in non-intrusive form, where access management application acts as a gateway and relays user requests to the managed platform. The following issues are important to consider when comparing access management solutions:

- Granularity of Access Rules

- Support of non-Web applications
- Resiliency and high-availability
- Interoperability with external devices
- Log and delegation management

Granularity of access rules – The more criteria are supported by the access rule the better business rules can be mapped into the application logic. The most common criteria of the access rule include but are not limited to user's IP address, group membership, time of the day, URL, UNC or other location and the nature of the resource being accessed, collection of credentials presented by the user, and specific business operation. Granularity of the operation access is very important in implementing Web portal and financial applications. The following scenarios can better illustrate the advantage of highly granular operation control: customers with over \$100,000 in their accounts can have real-time access to stock quotes, employees of the large customer of a health insurance company are automatically offered additional benefits based on the affiliate credentials produced when accessing the Health Insurance Portal. Ultimately, the ability to control information access in a highly granular fashion allows for efficient implementation of the business processes and decreases the burden on the development and security teams.

Support of non-Web applications is important for system support, engineering and custom application environments. The majority of the IAM solutions (especially Tivoli Access Manager) offer SDKs, APIs and sample code allowing developers to extend uniform LDAP-based access management to such applications as telnet, FTP and homegrown code. Usually, the proxy-based architecture is more efficient in securing non-HTTP application by acting as transaction brokers or protocol proxies.

Resiliency and high availability of the Access Management Solution are of the utmost importance. Architecturally, the IAM solutions are considered as keys to the kingdom. Thus, by rendering IAM solution nonfunctional, an intruder can completely block access to the protected resources even for the legitimate users. Similar situations can arise in the architectures with single point of failure. Therefore, Access Management Solutions should offer multiple levels of resiliency, such as: resiliency of the individual component, namely: management server, enforcement server, policy server, etc., and the ability of the plug-ins or enforcement servers to automatically fail over to the secondary policy server should the primary one die or get disconnected. From the security standpoint, the encryption of the communications and the encryption of the data in the data stores is a major advantage of the solution.

Interoperability with external devices – Applications like Oracle COREid Access and Identity (formerly Oblix NetPoint) can interoperate with firewalls to automatically fight DOS and brute-force password attacks by requesting firewalls to block a specific kind of traffic from a specific IP for a given duration of time. Such an event is reflected in the application log and in the security log of the firewall, thus alerting several teams to an attempted attack.

Such a behavior can be extended to application layer firewalls, XML firewalls and IDS systems. Not only does this feature simplify the protection against IAM attacks, it also leverages the investment into the existing security equipment and extends the functionality of such equipment to the application and IAM layer.

Log management and delegation management – Log Management allows administrators to monitor and get alerts on access events in a centralized fashion across multiple managed systems and policy servers. Delegation management offers secure delegation of a subset of access management functions to personnel with limited authority, training or skills. The feature also allows for the controlled subdivision of responsibility between the perimeter security team and the application management team.

Business Challenges

In modern enterprises the decision makers have to address the multiple challenges of the modern IT era, such as:

- With multiple identity stores and affiliate services, the number of changes can grow exponentially. Since access to sensitive information today is no longer exclusively granted to employees but to a wide range of outside entities, a flexible yet reliable method of granting dynamic and differential access rights is required. The dilemma between the desire to generate immediate customer and financial information and the requirement to enforce granular access restrictions creates difficulties for system and security architects.
- Multiple and inconsistent approaches to security services make it difficult to comprehensively protect business data, since authentication and authorization is usually handled by platform and application administrators, who do not share a common approach to data security. Office politics and tense relationship between different parts of an IT department may aggravate the situation.
- Digital security – which is no longer limited to traditional perimeter security, intrusion detection, or OS hardening – is gaining in importance. Identity provisioning and federation services have become more widespread and require unique methods of data protection. It is now fairly commonplace to install XML firewalls in order to supplement traditional perimeter defense, implement SAML-based application interoperability, and require IAM products to request security actions from firewall or intrusion detection systems (IDS).

With the need for hardware and OS upgrades on top of implementation of IAM solutions, the total per-employee cost of IT support is increasing. This is occurring in the face of decreasing IT budgets and staffing over the last several years.

To complicate matters more, enterprise boundaries are rapidly changing to include mobile workforces, customers, supplies, partners, affiliate services, offshore labor forces, outsourced HR and benefits vendors, outsourced application vendors, and many more.

In addition to internally-imposed security requirements, some industries (such as medical and banking) have to abide by a growing body of governmental regulations (such as HIPAA, Gramm-Leach-Bliley, the Sarbanes-Oxley Act, or the US Patriotic Act Customer Identification Program), which require that companies limit access to certain types of information to the appropriate people. Additional foreign or international regulations — such as International Accounting Standards (IAS), International Financial Reporting Standards (IFRS), European Data Protection Directive, or the Canadian Personal Information Protection and Electronic Documents Act — may apply to companies conducting business abroad.

Benefits of IAM Solutions

While it consumes both time and resources, the implementation of identity management offers a number of advantages, including legal, administrative, and security benefits. The specifics and significance of these benefits are discussed below.

Legal Benefits

Companies today must comply with a growing number of government regulations aimed at safeguarding consumer privacy, health and financial data, and e-commerce transactions. Foreign nations have also developed a number of government regulations governing data protection, which obliges multi-national companies to comply with both U.S. and foreign data protection requirements. In the wake of corporate scandals and intense media-generated pressure on governments, the number of data protection regulations is skyrocketing, requiring companies to adapt their data infrastructure on-the-fly to comply with the “latest and greatest” decisions of the legal and political communities. Each legal measure has specific deadlines and a large number of compliance criteria.

Legal accountability may require corporations to present data on system access, which can be difficult to obtain across multiple systems. Moreover, different systems may have different capabilities of authentication logging and access data as well as different policies on retention of such logs.

It has begun to dawn on companies around the world that implementing the complex set of technological data protection measures required to comply with all the regulations presents technical, administrative, and financial challenges. The problem may be aggravated by the need to completely redesign data-processing architectures and to re-train IT and clerical staff. Such implementation should not impede the core business objectives such as increasing revenue, improving the quality of customer service, and cutting IT costs. Companies are finding that implementation of a prepackaged Identity and

Access Management solution is the simplest way to ensure compliance. The approach has several benefits.

Firstly, it becomes an IAM vendor's responsibility to be appraised of, implement, test, and support the growing number of regulations, acts, and best practices. The vendor will be able to provide the risk analysis and develop and enforce security policies, many of which are also required by the government regulations. Choosing a proven security vendor provides confidence in senior management and limits legal liabilities by incorporating an industry-standard solution. It also simplifies the administrative and technical aspect of the rollout by relying on the vendors' experience with previous clients, experience that can safeguard against common mistakes and pitfalls.

Secondly, the IAM vendor provides the single point of responsibility, service, support, training (for user, developer, and IT communities) and product customization. With an IAM solution provided by a single vendor and composed of multiple products such as access, identity, directory, proxy, data vault, provisioning, monitoring, and other engines, the per-user cost of regulatory compliance is less than the multi-vendor solution. The single-vendor dependence can be an additional bargaining point to obtain product discounts and price reductions. Additionally, vendors that already have a foothold in the customer's enterprise in the form of hardware, directory services, network operating systems, or network management infrastructure can offer a non-intrusive implementation of the IAM strategy around the existing infrastructure, while preserving investment in the existing IT components.

Administrative Benefits

With the number of the business applications constantly increasing, it takes more and more time to provision user accounts. It is not uncommon for a newly hired employee to wait days or weeks for accounts on all business systems, including (but not limited to) local computer passwords, network passwords for file and print, firewall or proxy passwords, messaging system passwords, SAP/PeopleSoft passwords, timecard system passwords, UNIX passwords, mainframe passwords, remote access passwords, benefits portal passwords, etc. On top of that, there might be an additional collection of credentials for homegrown applications and a variety of hardware authentication methods. Such a situation not only increases the amount of training for senior and junior technical personnel, but also increases the Help desk costs, and decreases employee productivity directly (the time spent on the phone with the Help desk) and indirectly (the degree of frustration experienced in order to get things done). Also, differences in personal user information in multiple directories can create confusion and adversely impact productivity.

From the administrative point of view, absence of a uniform identity management solution creates major inconveniences associated with changing user accounts (updating personal

information, adding and removing permission, etc.) and deleting all accounts associated with a departing employee, especially in cases of acrimonious termination. The loose accounts still existing in the externally accessible system associated with a terminated employee constitutes a security compromise, since the firewalls and intrusion detection solutions deployed cannot block valid access to the system with a credential set that hasn't yet expired.

Centralized data storage eliminates duplicate identity data, increases the accuracy of user's personal information, and simplifies account management. From the security standpoint, the centralized identity architecture reduces the attack surface by decreasing the number of identity stores, enables the system to automatically disable and remove stale accounts and provides centralized logs of access and identity information.

Finally, auditing a user's access to all of the allowed systems cannot be performed in a centralized fashion, since the data has to be provided by multiple security administrators in multiple formats, and has to be consolidated and mined separately. Therefore, adequate enforcement of the corporation's policy on computing resource usage cannot be properly implemented. The same applies to the enforcement of uniform password strength and account lockout policies on heterogeneous systems.

From the security standpoint, consolidated information on the access denials across the enterprise as well as the ability to correlate all system across a given employee — e.g., Internet browsing patterns, access to shared resources, and remote access time and duration — could be of great assistance to security departments, especially to the application security teams, since this constitutes one key aspect of protection against internal intruders. Eighty percent of digital crimes are committed by the insiders, so a system offering uniform policy enforcement, auditing, reporting, and notification would pay for itself in a very short time, with the cost fairly spread against the budgets of the application and security divisions. The directory-enabled Internet proxy alone can save a corporation from a number of costly policy violations. The description of auditing and enforcement capability of such system alone (supplemented with the threat of disciplinary measures) could dissuade those who might otherwise abuse the computing policies.

Software Development Benefits

In order to enhance data availability, businesses commonly choose to web-enable in-house applications and hyperlink them across the Intranet offering full-fledged interoperability on the application level. With the availability of data via the web, verifying the identity of each user becomes very important. The issue is complicated if more than one authority must identify the users. Moreover, such an extension of the traditional application requires a large amount of custom code to be created.

An additional advantage of the IAM solution is the ability to separate the authorization of data access from the web application and to transfer such decisions into IAM. The IAM

solution enforces access policies across the enterprise in a centralized fashion and provides information to applications of the user's group membership. The managed application will only have to make the access decision based on the user group membership, as reported by the IAM.

In environments with centralized identity architecture, the development of identity-aware applications is faster than in an environment with disparate identity sources. Additionally, the availability of Software Development Kits (SDKs), Application Programming Interfaces (APIs), sample code, and consulting services from the identity solution vendors all make the in-house development process simpler and more efficient. A potential IAM vendor's partnerships and alliances, as well as support for common protocols and specifications, is an important criterion in choosing the IAM solution.

Security Benefits

After the events of September 11, 2001, the awareness of corporate security — including digital security — has been increasing. Additionally, those attacks forced the government to rethink security paradigms and increase security requirements, including relevant legal regulations.

It is well known that conventional security architecture composed of firewalls and Intrusion Detection Systems merely offer a limited amount of security, since most attacks have been initiated by malicious insiders through valid ports and application calls. Therefore, the issues of authorization and authentication governing the security of data have moved from the buffer overflow and protocol exploit level into the level of identity exploits. Maintaining a heterogeneous data security solution with 20-40 identity issuing authorities (application and operating systems) can lead to errors resulting in system vulnerability, since all accounts must be reviewed frequently against cross-corporate identity policies, the current employee database, and access inactivity periods. Consolidation of identity information with an IAM solution substantially reduces an enterprise's attack surface. Additionally, IAM vendors supply tools for security enforcement, authority delegation, and auditing of the IAM solution itself.

IAM solutions can further increase data protection by extending the functionality of the conventional OSEs and applications with hardware tokens, which are immune to password replays, brute-force password attacks, and end-user key- and traffic-loggers, since token-based security solutions require new authentication credentials to be presented every time. An IAM solution allows chained and step-up authentication to protect highly sensitive data. In these cases authentication with multiple form factors can be requested.

Finally, IAM solutions can be programmed to define and dynamically act upon certain access and identity events, and require additional authentication depending on the parameters of the data access, such as geographical location and business affiliation of the

user, time of day, and/or business nature of the transaction. For example, remote users performing transactions worth over \$100,000 can be asked to provide biometric authentication information. Interoperability of the IAM solutions and firewalls, as well as plans to offer IAM solutions such as XML firewall appliances, allows administrators to programmatically translate and enforce corporate security rules into the layer of business logic.

Financial Benefits

Since regular passwords are easily guessed or stolen, a single system access with stolen identity can expose large volumes of personal data or empower hackers with administrative access to compromised systems. Such identity-based breaches of security can cause companies massive financial and publicity damages. These potential threats can be eliminated by implementing a comprehensive IAM solution.

Whereas IAM security initiatives can be viewed by many as an unavoidable expense, it actually amounts to a solid investment in security, systems architecture, and customer service. The ROI of an IAM solution cannot be easily quantified, but can be approximated by calculating the combined financial benefits of reduced management effort and maintenance costs, increased reporting, decreased direct and indirect security risks, simplified end-user experiences resulting in higher revenue or productivity, full regulatory compliance, and a clear security roadmap. Additionally, the process of re-designing the security infrastructure, re-training employees, and restructuring architecture and business processes are better accomplished when not done under the pressure of damage containment.

Moreover, the deployment of state-of-the-art digital identity protection serves to increase user confidence in enhanced online business, encouraging repeat customers.

Market Requirements for IAM Solutions

In order to satisfy business needs, a modern Identity Management system should satisfy a number of essential requirements, which are summarized here.

Identity Solution Designed Around Business Policies

Although technology is an indispensable part of the Identity Management solution, the IAM should revolve around the business processes and procedures, since it is more efficient to redesign the underlying IT architecture rather than re-design business processes and retrain personnel. The solution should be business-driven, offering workflow mechanisms and customizable secure interfaces to all participants of the identity-handling process, in order to streamline user provisioning and to guarantee smooth end-user experiences while empowering the management and support personnel with the right amount of delegated management to eliminate potential system abuse.

Strong Authentication

Strong authentication reduces the risk of unauthorized access to data by increasing the computational effort required to forge the identity. Strong authentication goes the next step beyond password-based authentication (“what you know”), and includes token-based authentication (“what you have”) and biometrics (“what you are”). Strong authentication is of extra importance for remote data access, where the identity of the user cannot be verified by means of physical security. It is important for a potential IAM solution to support a large number of hardware token and biometric authentication approaches.

Federated Identity Management

Modern business requirements drive corporations to manage access to systems belonging to external entities, such as partners or outsourced services. In order to offer seamless but controlled access to data, employees should be required to authenticate only once to eliminate the need to remember multiple user IDs and passwords. This challenge is addressed by implementation of Single Sign-On (SSO) solutions using Federated Identity Management. In essence, SSO is based on trust, where one business entity provided a user with credentials which are in turn trusted by another business entity. This allows users to seamlessly cross the boundaries of corporate networks without losing accountability.

SSO not only eliminates frustration, increases employee productivity, and improves customer retention; it also maintains control over the employees’ personal data, since SSO does not require users to provide personal data to traverse borders into trusted portals and networks. SSO also decreases legal liability, since there is no need to control the compliance of corporate partners with data protection regulations. On top of legal and administrative advantages, SSO drastically decreases the IT overhead and the associated helpdesk calls.

A collaborative environment can be easily set up and configured through federated identity management; the alternative can be a nightmare. With federated identity management paradigm, your company is the only source of a user’s identity management information. The partners will receive limited information on a need-to-know basis at the time of access to resource.

An important factor in the analysis of the federated identity component of the IAM solution is the breadth of the vendor’s support for open standards, which may already be used by the organization’s business partners.

Ease of Implementation

Ease of implementation is of utmost importance, especially for large infrastructures. The IAM solution implemented should be able to leverage the existing infrastructure and IT investment (including directory services, file and print services, data repositories, security protocols) and to support major operating environments and business applications while

consolidating multiple sources of identity information. Additionally, the application should provide qualitative and quantitative reports having multiple levels of complexity for technical and administrative audiences. An IAM solution should require no client-side installation and be seamless and transparent to end-users.

To demonstrate compliance with the requirements set forth, the potential vendor should be expected to provide a pilot installation at the customer's site. The degree of effort required by the vendor to build, troubleshoot, and present such an installation is a good measure of the software quality. The customer must take into careful consideration such things as the number of servers required for demonstration, the number of vendor experts onsite, the duration of the preparation process, and the ability to troubleshoot and reconfigure the system on-the-fly. While a nice front end might appeal to senior management, addressing technical issues in a proper and timely fashion during the pilot project could win the hearts of senior IT personnel and, therefore, the seal of technical approval. It is also advantageous for the vendor to quote not only successful customers but also successful pilot projects.

Data Security

Issues of data security cannot be underestimated. It is important not only to encrypt user credentials in the data store, but also to provide adequate communication security between all modules of the IAM solution, including — but not limited to — communications taking place between the management console and the management server, the management server and the connector, the connector and the managed application or operating environment. The security department of a potential customer may not approve a solution where clear-text connection is established between the IAM product and one of the customer's systems. The implementation of standards-based strong encryption of data communications is a measure of the thoroughness of the IAM security solution. Practically, such thoroughness is best demonstrated when the proposed solution is composed of tightly integrated components natively provided by a single vendor, rather than cobbled together by means of mergers and acquisitions. In the case of acquisition, the elapsed time since it took place as well as the level of integration effort between the native and acquired code should be considered.

Resiliency

With multiple replicated authentication databases, a solution becomes more scalable and can be distributed geographically, across business entities, and across multiple networks and operating environments. In light of this, it is important for a considered IAM solution to offer high availability of all architectural components in the form of load distribution rather than a standby solution, with the ability to auto-configure clients in the event of unscheduled failover. Moreover, this high-availability solution should be native to the

application and not rely on external third-party components such as OS clustering and hardware application load-balancing.

If possible, the modules of the IAM solution should be capable of advanced problem diagnostics, self-repair, and crash-recovery.

In distributed environment resiliency also requires proper data transfer and event handling over slow WAN links. In the evaluation of the overall resiliency of the solution, attention should be paid not only to the resiliency of the individual components but also to the efficiency of the recovery scenarios offered by the vendor.

Manageability

The manageability of an IAM solution is one of the key factors that define its efficiency. Manageability is composed of several factors, each of which has different weight depending on the organizational needs.

Usually, the most important aspects of manageability include the following:

- Automation of the maximum number of administrative tasks
- Support of all models of administration (centralized, distributed, and user self-services)
- Workflow
- Centralized logging and auditing
- Web interface

In real life it may be insufficient to evaluate the manageability of a solution based on the vendor's brochures, sample business cases, and a live demonstration at the vendor's site or at a trade show. In order to gain better insight into the management capabilities of the IAM solution, a full RFP followed by a pilot installation on customer's site may be required.

Reporting Tools

Since the Identity and Access Management products generate a large number of logs, containing potentially huge amounts of data that tends to increase exponentially with increases in the number of users, directories, managed applications, and granularity of the access restriction, versatile log management becomes extremely important. Since IAM logs contain the result of authentication and authorization events, they constitute data not only of a performance and administrative nature, but of a security nature as well.

As such, the logs should comply with certain criteria. All architectural components should generate logs with multiple levels of logging and in a uniform log format. These logs should be securely transferred to the centralized management and monitoring station for data mining. In the event of temporary component unavailability, logs have to be collected on the component and be transferred to the management station upon reconnection.

The management server should have the means to automatically process and prioritize log events and to inform administrators in real time of critical system and security events. The management server should offer an interface to mine the logs and to create pre-defined and custom reports based on a number of parameters. Additionally, logs should be presented or exportable to a large number of formats for the purposes of offline storage, post-processing, and presentation. Finally, the management console should display the status (availability, health, and load) of each component of the IAM solution for the operations staff.

The monitoring and reporting capabilities of the proposed IAM solution have to be carefully reviewed by the operations staff to evaluate the effort required in the solution's day-to-day management.

Support of Standards

In order to interoperate with other security solutions, the IAM solution should fully support open standards such as Security Assertion Markup Language (SAML) and the Liberty Alliance specifications including Identity Federation Framework (ID-FF). Additionally, supporting upcoming standards such as WS-Security, WS-Trust, and WS-Federation is a big plus for a security solution vendor. It also make sense to discover whether certain alliances and standards have been created and/or maintained due to the particular vendor's initiative, since this gives some indication as to whether or not the potential vendor can lead and remain a *de factor* standard in the IAM arena.

Tools and Utilities

Often vendors supplement their solutions with a collection of tools and utilities that simplify troubleshooting, allow protocol and application debugging, offer interoperability with other applications on the protocol, command or log level, simplify scripting procedures, provide bulk data import and export. Additionally, vendors will supply SDKs with API sets in C++ or Java (usually both), sample code with comments, sample forms and report templates. Some vendors go as far as offering a sample site, which illustrates the implementation and functionality of a given IAM solution.

Completeness of the Solutions

It is to the potential buyer's best advantage to obtain a homogenous IAM solution from a single vendor rather than purchase bits and pieces from different vendors and then face the complex challenge of getting the acquired components to interoperate. In order to evaluate the completeness and internal integrity of a considered IAM solution, the following aspects of the potential vendor's business must be considered:

- How long has the vendor been on the market as an IAM solution provider?

- Does the vendor rely on its own technology for all components of the IAM solution, including (but not limited to) data storage, directory services, and workflow?
- Has the vendor recently obtained through acquisition new technology that it now must incorporate into the existing portfolio of products? If so, how soon following acquisition was the new roadmap proposed? How thorough and timely has the integration process been? How carefully did the vendor merge different technologies – especially in the areas of centralized management and logging? Finally, how were the existing customers of both solutions treated during the migration process?
- Does the vendor offer user-centered services beyond IAM, such as directory-based proxy or portal solutions?
- Can all the vendor’s products be centrally monitored and centrally managed through a uniform set of GUI- and web-based interfaces?
- What is the overall installed base of the vendor’s product (millions of seats)?

Overview of the Market Players

The Identity and Access Management (IAM) market had developed over the past half decade as the issues of identity management became mission-critical. The Identity and Access markets somewhat overlap because vendors break their solutions down into access, identity, federation, and meta-directory components. This allows vendors to slip into the customer’s infrastructure and decrease the implementation cost by offering components interoperable with currently installed solutions from other vendors. Additionally, the sale of one or two IAM components to a particular customer opens the door to selling additional IAM and non-IAM products to the same customer.

Numerous reviews, reports, and other pieces of research have been published to cover the IAM market. One way to present the competitive stance of vendors is to plot a “magic quadrant”; a two-dimensional representation of the market with the “Presence” and “Performance” as axes. A magic quadrant is a simple representation of the current state of the market that provides very limited information in a generalized fashion. We believe that it is more important to concentrate on the efficiency, completeness and the maturity of the vendor’s architecture. Additional important features to be addressed are the overall development strategy of a vendor, recent acquisitions, levels of product extensibility, as well as support and adherence to its own roadmaps and proclaimed release dates.

Following is a brief summary of the characteristics of current IAM players.

IBM/Tivoli

Tivoli, a subdivision of IBM has been an IAM player for the number of years. Tivoli products are aimed at large customers with distributed computing facilities. Tivoli products usually require Tivoli Framework as the underlying infrastructure. While Tivoli offers a reliable, scalable, and robust solution, it is often difficult to implement because of

the large initial implementation stage, large number of manual operations, lack of uniform centralized logging and a limited friendliness of the user interface. Tivoli is constantly updating its products and recently supplemented its portfolio with Directory Integrator, a meta-directory solution, which acts as a directory broker. While Tivoli supports more features that could possibly be needed, the initial implementation and IT training steps are very time- and funds-consuming, making the application of limited applicability to small customers.

Sun/Waveset

Sun/Waveset is yet another example of an acquisition of a small IAM software company by a large corporation for which identity has never been a priority. Whereas Waveset is a simple and robust application with limited feature set, Sun is known for the limited success with the implementation of the acquired technologies (Cobalt) and mixed roadmaps (x86 Solaris, Linux on Sun hardware, Gnome desktop). Currently it required a major development effort to achieve interoperation between Sun's own IAM solution and Waveset Lighthouse, which uses a less efficient virtual directory approach. As of this writing, no clear roadmaps are available, and both Sun and Waveset products are being offered to customers in parallel.

CA/Netegrity

The recently acquired Netegrity IAM SiteMinder-based suite adds substantial value to CA's own eTrust-based solution. To everybody's surprise, CA offered realistic and firm plans to incorporate Netegrity technology with its own products, by identifying and eliminating duplicate products and turning the rest into a versatile offering under a uniform monitoring and management umbrella without the loss of functionality and supported platforms. The offering resulted in a dozen of products that address the entire IAM spectrum. According to recently published roadmaps, the entire merge should take less than two years, with the results of the first stage being available as we speak.

Novell

Novell entered the IAM space long ago by introducing one of the first directory-based NOSes. With the need to connect disparate Windows systems, Novell had to deal with access and identity issues from day one. The core of the Novell's solution is the robust and scalable eDirectory acting as a data vault, and Nsure identity management solution. Novell offers drivers for major OSes, directories, and applications. Additionally, Novell features fast and simple product implementation. On top of the IAM solution, Novell offers additional directory-based components such as iChain, Border Manager, etc., that can handle other issues of authentication-based information access.

HP

HP is trying to enter the IAM arena by extending OpenView with Select Access and Select Identity components, which were obtained by acquiring two small software companies. Select Access and Select Identity are relatively new to market, so it is difficult to evaluate the completeness and the depth of the approach. However, given the limited prior interest in the IAM space and the need to fully integrate the separately acquired components, HP solution is likely to present a limited advantage to potential customers. HP has never been known for its directory or user management products. Also, with the recent change of the CEO and the need to increase the sales of server and storage hardware, the IAM momentum can easily be under funded or mismanaged. Edison Group is endeavoring to learn more about HP's Identity and Access Management solutions. This document will be updated to reflect that research.

Microsoft

Microsoft is a relatively new player in the IAM space. The vendor is trying to heavily compete in yet another market (OS – NOS – Messaging – RDBMS – Browser – Office Suite - Application Server – world domination?) with the MIIS virtual directory product and interoperability with IAM components from other vendors, such as RSA. Given experience with other Microsoft products, the IAM solution won't be stable, documented, and reliable in at least Version 2 Service Pack 1. However, the major advantage for Microsoft is compatibility with the large Windows installed base and the introduction of IAM standards into Windows and the Active Directory API set, which will allow for the development of IAM-enabled applications (which may not necessarily be compatible with the rest of the standards from the non-Microsoft world).

Oracle/Oblix

With the acquisition of Oblix, Oracle is trying to enter the IAM arena. Despite impressive corporate finances and aggressive business practices, it will take Oracle several years to fully develop the Oblix suite of products and to integrate it with Oracle product line, such as its RDMBS and application server. With the recent acquisition of PeopleSoft, Oracle's finances, priorities, and development effort might be diverted from the IAM playing field. Alternatively, with Ellison's tenacity, finances and marketing muscle, Oblix technology can get a major boost. The next six months will tell us which prediction is more accurate.

Summary

The extensive set of requirements described here makes it clear that the choice of vendor is critical in the success of an IAM initiative. Vision and strategy is required of an IAM vendor; more specifically, the vendor must demonstrate an ability to offer a thorough and dynamic data protection solution that can be implemented around the existing business processes and technologies, yet deliver an adequate level of security through a simple set

of customizable management interfaces. To satisfy such requirements, a potential vendor should have extensive expertise in managing millions of users in distributed environments, where issues of administration delegation, directory interoperability, credentials management, and resiliency must have been tuned to perfection through multiple versions of the product, a large installed base, and many successful operations. A good indicator of a solution's completeness is its ability to handle the most common access and identity situations arising with a heterogeneous installed base and specific business requirements.

The implementation of an IAM solution usually undergoes the following stages:

- identification of the requirements
- brief market overview, identification of the potential vendors
- creation of the extended FRP that addresses both technical and non-technical issues
- discussion of the obtained responses
- meetings with the potential vendors (on-site, at vendor's demo lab and with one of the featured vendor's customers)
- pilot implementation of the vendor's solution on at the customer's site
- planning of the rollout upon the successful performance of the pilot version
- implementation of the IAM solution
- applicable training, documentation, brain dump
- ongoing vendor support and application customization

This Business Strategy Report can only provide an introduction to the challenges facing enterprises dealing with identity and access management solutions. Edison Group analysts are available in our usual role for the vendor community as well as providing decision making support for enterprises making acquisition decisions. Please contact Edison Group at Consulting-Services@theedison.com to for more information.