Identity and Access Management Defined

An IAM solution requires multiple products from multiple vendors. It also results in business process change. Obtain senior management support and phase in the IAM implementation according to your "pain points."

Managing user accounts and privileges — user access management — isn't getting easier. The related "enterprise directory" project has proved to be an elusive goal. As enterprises externalize their business processes over the Internet to customers and trading partners, they have expanded the number and types of users with which they must contend. Accordingly, more users need access to IT resources; platform environments will remain complex and heterogeneous; and Web services are driving the need to manage transactions, as well as user access to IT resources. Thus, enterprises no longer can effectively manage user access to the heterogeneous IT environment (for example, external and internal user identity information repositories, databases, operating systems, and applications) for multiple access purposes, such as business roles, password management rules and business hours access policies.

Directories and platform-specific security administration products can't address all of the demands of a well-managed and automated security administration function. Therefore, a range of other technologies, including user provisioning and extranet access management (EAM) products, have evolved to address enterprises' growing need for user account and privilege administration. No product does everything — user account management, privilege management, password management and single sign-on (SSO) — across all platforms and for all application types. A multiproduct implementation is the only way to meet these enterprise requirements. Vendors are addressing this multiproduct approach by delivering identity and access management (IAM) product suites.

The Four "A's" of Information Security
Enterprises need to ensure that users are properly identified and that these identities are validated to IT resources — this is *authentication*. They need to know that users can only access what their job function allows them to access within the enterprise — this is *authorization*. They need to have a consolidated, enterprisewide view and way to manage user access — this is *administration*. Finally, they need to ensure that the activities associated with user access (administration and real-time enforcement) are logged for day-to-day monitoring, regulatory and investigative purposes — this is *audit*. These four "A’s" of information security (see Figure 1) will be delivered by emerging IAM technologies.

Interest in IAM grew rapidly in the first half of 2003. For fiscal 2003, the IAM market is forecast to have a compound annual growth rate of 12 percent, according to Gartner Dataquest.

**Administration Through Identity Management**

IAM solutions solve two main functions: administration and real-time enforcement. Identity management solutions address enterprises’ need to administer (create, modify and delete) user accounts, user profiles and corporate policies across the heterogeneous IT environment via a combination of user roles and business rules. Also included as part of administration activities is the capability to abstract and automatically correlate

---

**Figure 1**

(User Identities, Transactions, Roles, Policies and Privileges)
data from HR, customer relationship management and e-mail systems (and other “identity stores”), and from the managed systems. Fulfillment is accomplished in a variety of ways:

- In response to a self-service request — for example, self-registration
- A line management request — for example, the manager has a new employee who starts work on a certain date or a user needs access to an application
- A change in an HR system — for example, employee termination
- A bulk load for purposes of a new application or merger/acquisition

These activities must be monitored for regulatory and investigative purposes.

The markets and associated functionalities within identity management are:

*Password management* includes simplified help desk password reset, self-service password reset and password synchronization, including bidirectional synchronization. Password synchronization can be a problem for the information security organization because if the single password is guessed by a hacker, then he or she has access to many more applications than if there was a unique password for each application. This could cause more harm. However, the information security organization’s resistance to password synchronization can be overcome if the password formation, history and retention capability of the password management product can provide a stronger password management position enterprisewide.

*User provisioning* encompasses user account management (create, modify and delete user accounts and privileges) for access to the heterogeneous IT resources. Enterprises typically use user provisioning to manage internal user access. User provisioning products act as the single point of administration for legacy and client/server application environments, as well as corporate utilities such as e-mail. Most user provisioning products offer password management functionality, delegated administration, a role-based access control model, workflow (a distinguishing feature from earlier consolidated security administration products) and automated fulfillment of the access request. Some products offer synchronization of user profile information among authoritative sources of user identity information.
Metadirectories include user account management (create, modify and delete user accounts and privileges) for access to the authoritative sources of user identity information. Metadirectories also provide data accuracy and precedence for those user identity repositories, as well as synchronizing the user profile information. Historically, metadirectory products have lacked functionality such as password management, role management and workflow, which are standard functions of user provisioning products. Starting in 2001, metadirectory vendors have rounded out their offerings and are starting to look like user provisioning vendors. By 2005, the capabilities of metadirectories will have merged into user provisioning products and there will be only one market for user provisioning products (0.8 probability).

Real-Time Enforcement Via Access Management

Real-time enforcement is addressed by access management solutions that can enforce, in real time, an access control policy (or policies) for each user of enterprise IT resources. The two information security activities involved in the real-time enforcement process are authentication and authorization. Users must be identified, their identities must be validated, and a decision must be made whether they are authorized to access the requested resource. Some enterprises must perform dynamic authorization to resources based on the status of the user at the time of the access request. For example, if a customer has purchased more than $500,000 worth of merchandise within the past 12 months, he or she gets access to platinum-level services (for example, free shipping or financing options). The customer who has purchased only $200 worth of merchandise within the past 12 months must pay for shipping and must use a credit card.

The markets and associated functionality within access management are:

Authentication services help identify users and validate their identities. This area contains multiple markets:

- Directory services store user identity information, include technologies such as LDAP, X.500, relational databases and others.
- Virtual directory technologies can be used to ease the administration and real-time authentication problems of user identity information that is being stored in many repositories, each with its own schema and owner.
- User authentication products, such as public-key infrastructure, tokens and biometrics, provide multifactor identity validation.
SSO products enable a user to access multiple computer platforms or applications after being authenticated with a single password. SSO products support interenterprise and intraenterprise SSO for non-Web applications (complex because of the need to manage multiple authentication protocols) and Web applications (simple because of the common authentication token known as a "cookie").

Federated identity services, which are best defined by the Liberty Alliance and Microsoft Passport, provide a "trusted" authentication environment. The enterprise that is being asked to grant access to the user (the "consumer") can trust the user identity information provided by the user's initial authentication service (the "producer").

Authentication management infrastructure products offer a single "authentication gateway" to target systems. The gateway supports a variety of authentication technologies. It requests the user to provide the appropriate authentication method based on the requirement of the application being accessed.

Enterprise access management is the real-time enforcement for authorization to an IT resource based on an access policy. Enterprise access management also comprises multiple markets:

- Operating-system access enforcement is delivered through products such as RACF, CA-ACF2 and CA-Top Secret for the mainframe, native platform access control services and third-party products for AS/400, Unix, NT and others.

- Database row and column access is provided by products such as Oracle's Label Security.

- EAM, also known as Web access management, offers integrated IAM for Web-based applications. Initial implementations focused on external user access. However, the growing use of portals for employee access is also driving demand for EAM solutions. Most products offer self-service password reset, delegated administration (including user self-service), a role-based access control model, workflow and automated fulfillment of the access request.

Functional Overlaps

There is functional overlap in the area of administration for IAM products. IAM products need an interface to manage the product and to add, modify and delete users, as well as some level of delegated administration. User provisioning and EAM products have further overlap in the areas of workflow, role management, delegated administration and password management.
Enterprises are looking for one interface to manage all user access to legacy and client/server applications and Web-enabled applications — regardless of the user's relationship to the enterprise. Thus, vendors in the user provisioning and EAM markets are providing such functionality at an abstracted level that Gartner calls identity administration. Identity administration functionality is provided through a common console that can direct the user provisioning and EAM products to fulfill on the access request. By 2005, where user provisioning and extranet access management products are both implemented, identity administration will be performed by a common administration console (0.8 probability).

The Future of IAM Markets

More vendors are offering more components in the overall IAM solution stack because the activities of the IAM markets are related to the management of user access, and enterprises want to manage user access from a common, integrated facility. Vendors such as IBM/Tivoli, Computer Associates International, Novell, RSA Security, Entrust and Netegrity offer integrated products in the two main areas of IAM: user provisioning and EAM. Through 2005, more vendors are expected to do the same at the risk of being shut out of the IAM space altogether.

**Bottom Line:** Identity and access management solutions are a growing "must have" for enterprises of all sizes and industries. Knowing which product to start and end with in the overall implementation, and why, can help reduce the investment in providing you with a secure access control infrastructure. You should:

- Phase in the implementation based on your most pressing "pain point(s)" — for example, directory services proliferation vs. growing help desk costs for password management vs. failed electronic data processing audits for security administration.

- Establish a road map for long-term application integration — analyze the resources required to integrate homegrown or commercial off-the-shelf applications to ensure business value.

**Acronym Key**

- **EAM** extranet access management
- **IAM** identity and access management
- **SSO** single sign-on