Identity and Privacy Strategies

In-Depth Research Report

Enterprise Identity Management Market 2006–2007: Not a Winner-Take-All Market

Version: 3.0, Nov 06, 2006

AUTHOR(S):

Mike Neuenschwander
(miken@burtongroup.com)

TECHNOLOGY THREAD:

Identity Management

Conclusion

The identity management (IdM) market is a fast-growing space focused on some of today's most pressing technology issues: digital identity, privacy, security, authorization, and account management. The criticality of identity technologies is not lost on the world's largest software vendors, most of which now have IdM strategies and products in hand. Given the nature of the market, vendors will find it difficult to dominate the space, and so many areas of IdM will remain hotly contested in 2007. During this period, enterprises must forge ahead with IdM projects to better secure online resources, comply with regulations, and reduce operational costs.

BURTON GROUP 7090 Union Park Center · Suite 200 · Midvale, Utah 84047 P 801.566.2880 F 801.566.3611 www.burtongroup.com

Publishing Information

Burton Group is a research and consulting firm specializing in network and applications infrastructure technologies. Burton works to catalyze change and progress in the network computing industry through interaction with leading vendors and users. Publication headquarters, marketing, and sales offices are located at:

Burton Group
7090 Union Park Center, Suite 200
Midvale, Utah USA 84047-4169
Phone: +1.801.566.2880
Fax: +1.801.566.3611
Toll free in the USA: 800.824.9924
Internet: info@burtongroup.com; www.burtongroup.com

Table Of Contents

Synopsis

The identity management (IdM) market continues to attract investment from top-tier software vendors and to provide a healthy environment for startup companies. The market has grown so large, so quickly that it's often difficult to draw clear boundaries around the market space. Some products, such as IdM suites, are easily categorized. Nearly all major software vendors offer IdM suites of varying breadths. EMC also recently acquired RSA Security, giving EMC some properties in the IdM market space. This “front guard” of major software vendors has invested significantly in the IdM market—mostly through acquisition—and now benefits from strong growth: Some of the companies claim (unofficially) greater than 30% growth in their IdM business.

These vendors' appetite for acquisition hasn't left the IdM market bereft of startups, however. Rather, it has cleared the way for a new generation of startup companies to emerge and for many remaining startups to flourish. New product categories are appearing, including audit and regulatory compliance tools, user-centric identity applications, consumer authentication products, fine-grained authorization and role discovery tools, and identity-aware appliances. The number of market participants continues to grow, with more than 90 vendors offering IdM-focused products.

The most significant development in the IdM market over the last year, however, is the emergence of frameworks for broad identity exchange. While Microsoft continued to blaze a trail with CardSpace (formerly InfoCard), IBM and Novell announced their support for Project Higgins. A broader group of vendors is working to create an Open Source Identity Selector (OSIS). New identity protocols are also emerging to support Internet applications, such as blogs. Although these initiatives are in a fledgling state, taken together they represent an industry-wide movement toward improved use of identity on the Internet and in corporate environments. They may also provide better frameworks for developer access to identity information.

As Burton Group has said before, IdM is no longer just a good idea—it's imperative. Business technologies cannot be built solely on the basis of anonymous communications. Given the urgency of the drivers for IdM, enterprises must move forward with the tools at hand. Fortunately, many IdM products are mature, valuable technologies that help enterprises make evolutionary steps toward identity-enriched online systems. As enterprise information technology (IT) departments grapple to reduce risk, thwart attacks, comply with regulations, and instill confidence in customers and partners, the discussion inevitably leads to improving the infrastructure for digital identity.

Analysis

The identity management (IdM) market continues to enjoy phenomenal growth—both in terms of sheer capital invested in the market and in awareness of IdM in the popular consciousness. Top-tier software vendors continue to fuel the market through investment in research and development (R&D) for their existing products, ongoing acquisition of boutique IdM vendors, and contributions of intellectual property to standards bodies and open source projects. Many IdM-related concerns have gained the attention of government and the media, making identity a topic of social import.

The undercurrents responsible for the IdM market's dramatic growth are nowhere near exhaustion, enabling the IdM market to continue on its growth path for some time. Large-scale issues ranging from identity theft and public safety to business trust and corporate accountability are symptomatic of an online infrastructure pushed beyond its design parameters. The general anxiety over exploitation in online environments is a critical driver for IdM technology. In reaction to public and governmental demands, the technology industry has produced a wide range of solutions aimed at improving confidence of online users. And as businesses continue to look for greater efficiencies while securing critical resources, identity-based access systems are becoming essential to enterprise infrastructure.

The IdM market is healthy and growing—with annual software sales in excess of $1.5 billion in 2005. But it is also an extremely difficult market to corner. To date, there is no clear all-out winner in the IdM market and the list of contenders continues to grow. In fact, the path of the IdM market defies many of the traditional hallmarks of technology market growth. The market has resisted private ownership, proven problematic to standardize, and drawn a disproportionate degree of governmental regulation. In short, unlike many of its closest neighbors, the IdM market isn't a winner-take-all market. In the IdM market, vendors compete in a commons, making it difficult to capture a controlling share of the market. Accordingly, technology vendors' need to arrive at strategies for endurance in this wide-open market has had a significant effect on the market in the last year.

Many vendors have shifted their focus from strictly IdM technologies to solutions for compliance and audit. These solutions include identity-enabled forensic and reporting tools as well as stronger authentication technologies. The scope of these solutions also stretches well outside traditional enterprise boundaries. For example, in the wake of the Federal Financial Institutions Examination Council (FFIEC)'s guidance on Internet banking, several vendors began targeting low-cost-of-entry consumer authentication solutions.

The IdM market is also increasingly intersecting with the information technology (IT) management market. Vendors with significant management brands, such as BMC Software, CA, Hewlett-Packard, and IBM, continue to emphasize the management aspect of identity management. IdM suites from management vendors are blending with IT Infrastructure Library (ITIL) architectures and are beginning to support configuration management databases (CMDBs). However, the integration work is only just beginning. These companies are building compliance solutions that rely heavily on technologies from both their traditional management businesses and their IdM suites.

An increasing number of vendors are also looking to segmentation strategies to bring their IdM portfolios into a more defensible position. For the first time in the history of the IdM market, vendors have successfully targeted small to mid-size businesses (SMBs). Vendors are also beginning to offer editions of their products for specific verticals, such as the financial, healthcare, and manufacturing industries and for local and national governments. Some vendors are able to market directly to these groups, but many are partnering with professional services firms to provide both the industry expertise and the delivery channels.

Amid this struggle for vendors to find continued relevance in the IdM market, a new generation of frameworks, developer tools, and standards are appearing that bears only faint resemblance to the previous generation. Until recently, the majority of the standards and open source work in the IdM space derived from the Lightweight Directory Access Protocol (LDAP) standard. With the appearance of Security Assertion Markup Language (SAML), the industry began shifting its focus from directory access standards to interoperability of identity information. This year, initiatives such as CardSpace, Project Higgins, and Open Source Identity Selector (OSIS), as well as a number of proposed identity protocols, represent a complete departure from the industry's LDAP legacy. Though early in their development, these technologies represent a wholesale reconstruction of IdM, based on new data models, broadly scoped information protocols, and more accessible developer frameworks.

As the IdM market continues to take on Internet-scale and societal issues, it's also becoming clear that the current IdM style prevalent in enterprise networks isn't always suitable for intradomain environments. Accordingly, alternative styles are emerging that afford communities sufficient safety and security without requiring centralized management schemes. (For more information, see the 2006 Catalyst Conference North America presentation, "Thinking Outside the Domain: The Emergence of User-Centric Identity and the Trend Toward Pro-Social Management Systems.") The emerging style de-emphasizes pre-issuance vetting of identity, reliance on structural controls (such as access controls), and centralized administration, while emphasizing recognition, collaboration, and reputation. Elements of these styles are already in use at large Internet sites (for more information, see the *Identity and Privacy Strategies* Methodologies and Best Practices [MBP] document, "A Review of Identity Practices in Internet Communities").

The Identity Difference: Not a Winner-Take-All Market

The high-tech market is known for its spectacular displays of winner-take-all market forming. Winner-take-all markets have a formulaic development, generally in three acts. The drama begins as a number of early entrants draw attention to a business opportunity. Once it's clear there's a great deal of money to be made, the competition intensifies as vendors fight to become the dominant vendor in the market space. And once a vendor gains sufficient momentum, the majority of the market consolidates around the vendor, starving all but one or two competitors out of the market. Operating systems, browsers, e-mail servers (and clients), enterprise resource planning (ERP) systems, databases, and routers have all followed such a course.

The centralization of rewards in winner-take-all markets dramatically affects vendor behavior. The potential for an extremely large payout draws the attention of top-tier vendors (which are generally previous winners of a winner-take-all market). Furthermore, vendors win not just by getting more business, but by ensuring that every gain they make is a loss to their competitors.

The IdM market has so far resisted winner-take-all dynamics, although vendors remain locked in that mythos. For example, when Microsoft and Netscape released their directory services, it seemed that the entire directory market would consolidate around one of those vendors. But in 2006, there are still more than half a dozen significant providers of directory services (including CA, IBM, Microsoft, Novell, Oracle, Siemens, and Sun Microsystems). Provisioning systems have been on the market for half a decade and the number of vendors in the space continues to grow (currently, there are more than two dozen provisioning vendors). Cornering the authentication market by now seems a mathematical impossibility; the space is heavily nuanced with a wide range of technologies and vendors. And even IdM suites—the ultimate attempt at consolidating the market—hasn't produced a clear winner yet: In 2006, customers have at least a dozen IdM suites to choose from. Today, there are close to 100 vendors in the IdM market (see Table 1)—more than ever before—and the market continues to grow. The 2006 vendor list is larger than last year's by about 40 companies, partly because this year's list now includes identity-aware appliances. But many startups have arisen in the "traditional" IdM space as well, particularly around policy services and role management solutions.

Although vendors continue to approach the IdM market as a winner-take-all proposition, features of IdM make the market extremely difficult to dominate. For one thing, the resources that identity vendors aspire to control are politically fragmented, physically distributed, and technologically diverse. No vendors to date have shown the resourcefulness and the will necessary to provide sufficiently broad interoperability to manage such a wide range of resources. In fact, vendors with the most resources have little political motivation to provide IdM for legacy or competitive products, because it's more to their benefit to replace those systems with their own.

But a more important reason that IdM resists winner-take-all outcomes is that identity information behaves as a common-pool resource (CPR). IdM plays in a space where resources are shared, as in a commons. Better analogues for the IdM market, then, are other CPRs, such as energy, water, and open water fisheries. One of the hallmarks of CPRs is their difficult and costly exclusion—that is, they're difficult to put fences around. (For more information, see the *Identity and Privacy Strategies* overview, "Thinking Outside the Domain: Revisiting the Function of Identity Information Across Digital Communities.")

The ramifications of a CPR market are significant. A CPR market presents the industry with a social dilemma, in that market participants are unlikely to collaborate, even though such collaboration would produce the best result for everyone. But as vendors continue to wrangle for control of the IdM market, no clear winner will emerge. Interoperability will become critical to success in solving the wide range of identity problems, but it will be extremely difficult to arrive at. Accordingly, government intervention will become necessary to break the stalemate.

Market Definition

The IdM market includes the set of technologies and products that enable the use of digital identities. Today, a great many products deliver such functionality. In particular, the IdM market consists of technologies that enable authentication of participants and authorization of transactions among users and online resources, as well as the administration of user accounts in online systems. IdM is the intervening, enabling, and validating infrastructure for managing interactions among subjects (such as users and services) and resources. (For information on IdM concepts and functions, see the *Identity and Privacy Strategies* Root Document, "Enterprise Identity Management: Moving from Theory to Practice.")

Figure 1 categorizes IdM products into four functional areas: authentication, authorization, account management, and validation. Authentication and authorization are runtime services that control the access and interaction with resources for each session. These services rely on back-end systems that are set up in advance of the session by user management products. The management and audit layer is a comparatively recent product category. Validation products report the actual behavior of the system and how that behavior differs from policy. Validation products also maintain records for forensic purposes. Products in this class also provide general monitoring and operational management of the IdM system itself (rather than the administration of IdM policy).

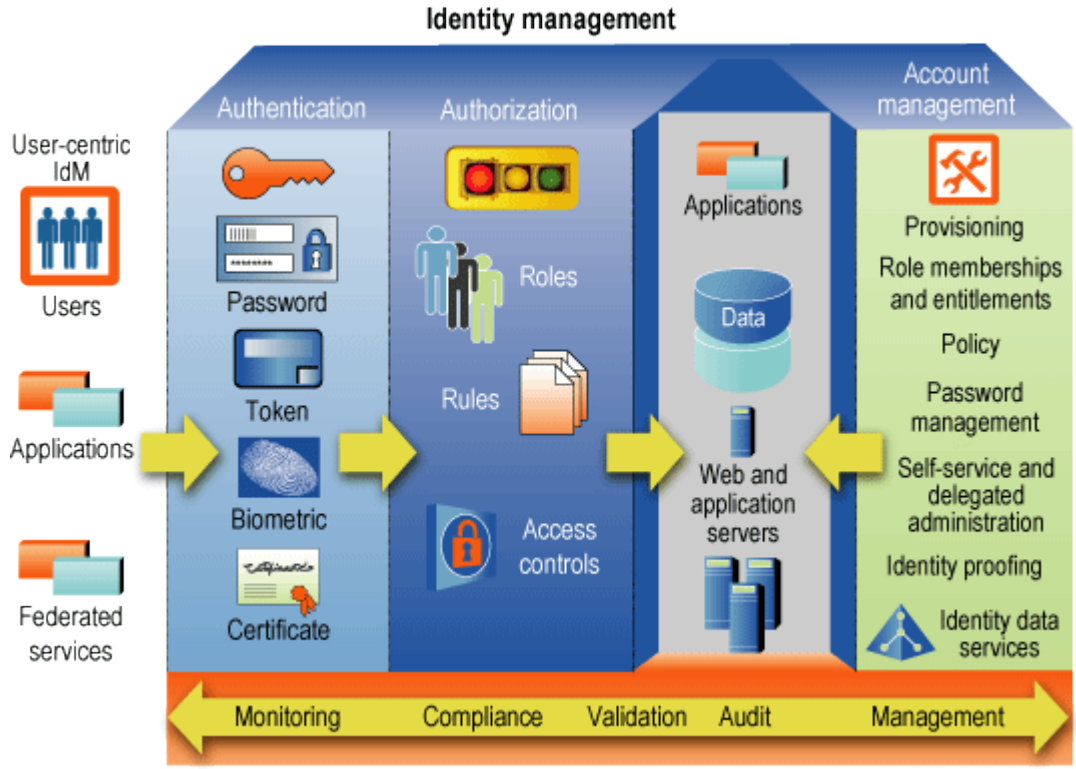

Figure 1: *Categories of IdM Products*

Relative Value by Category

Although each of the four categories of IdM is an essential component of a state-of-the-art IdM infrastructure, these categories differ significantly in market value.

The authentication space offers vendors potentially high returns, but the pain point (the degree of difficulty in deploying products) remains high enough that mass adoption of stronger technologies remains out of reach for most purposes. However, new mandates, such as the FFIEC guidance, help move the industry toward adoption of stronger authentication technologies (for more information, see the *Identity and Privacy Strategies* overview, "Consumer Authentication and the FFIEC Guidance"). In addition, the demand continues to rise for enterprise single sign-on (ESSO) products, particularly in conjunction with stronger authentication systems. Stronger authentication product vendors, such as DigitalPersona, SAFLINK, ActivIdentity, and RSA Security, are therefore moving "up market" to provide ESSO solutions that address some of the integration challenges. Nevertheless, much of the value of these segments remains untapped. (For more information on ESSO, see the *Identity and Privacy Strategies* overview, "Strong Authentication: Increased Options, but Interoperability and Mobility Challenges Remain.")

In contrast, the web single sign-on (SSO) market blossomed and then approached commodity status quite rapidly. After early entrants, such as DASCOM (acquired by IBM) and Netegrity, proved the value of the space, more than a dozen vendors subsequently proved the repeatability of the technology by entering the market. Vendors attempted to sustain the margins on these products by creating sophisticated authorization engines, but in the end, most customers wanted these products for their SSO and coarse-grained authentication features. Web access management (WAM) remains tremendously popular, but margins for vendors are reaching commodity levels and prices are vastly similar across competitive offerings. Sun's pronouncement to the market at the 2005 Catalyst Conference North America that it would open source its web SSO product seemed on some level a commentary about the web SSO market segment. (For more information, see the *Identity and Privacy Strategies* report, "Web Access Management: Surviving Maturity.")

Demand for federation products invigorated the authentication segment over the last year, but the uptake of federation has been measured. Many vendors are pursuing federation products as a stand-alone product category, while other vendors are integrating federation into their WAM products. BMC, CA, Diamelle, Novell, Oracle, and Sun provide both federation-enabled WAM and stand-alone federation products. Federation technology is becoming integral to many other products, including authentication technologies, Secure Sockets Layer (SSL) virtual private networks (VPNs), ESSO products, virtual directories, Extensible Markup Language (XML) security and management products, and ERP applications. (For more information, see the *Identity and Privacy Strategies* report, "Federation Products: Building Blocks of a Growing Federation Ecosystem.")

Policy enforcement as a separate product category is still emerging. In most cases, products in adjoining categories provide role, rule, and access control infrastructure. Startups are emerging around fine-grained access control and role discovery, but although interest in these technologies is high, the value of the space remained low in 2006.

Similarly, most products for IdM validation are still maturing, so although the market holds the promise of enormous value, in 2006 the adoption has been moderate. (For more information on validation technologies, see the *Identity and Privacy Strategies* report, "Achieving Organizational Compliance: The Emerging Role of Identity Audit Software.")

Much of the monetary value in the IdM market remains in the account management segment, which includes provisioning, meta-directory services, password synchronization, and user self-service products. Not surprisingly, the category is quite crowded, with several dozen vendors providing products in the space. But even though many of these technologies have been in the market for years, user management remains popular and margins have so far evaded commoditization. Unlike SSO, user management offers room for technology expansion, particularly in eroding the ratio of software products to professional services. Also, user management technology has proven to be expensive to mimic, especially because of its ties to process (which aren't easily encoded in a product). For more information, see the *Identity and Privacy Strategies* Market Landscape document, "Provisioning Market 2006: Urban Sprawl in IdM's Most Livable Space."

Market Participants: A Review of IdM Vendors

The IdM market has matured to the point where the business model associated with a particular brand is the key differentiator. Similar to a shopping mall, as depicted in Figure 2, IdM vendors approach the market from any of three business models. *Anchor brands* are marquee vendors that, like department stores, offer a wide variety of products. As such, each of these brands represents multiple product categories rather than a specialization in a particular space. Eight vendors currently fill this role in the IdM market: EMC (RSA), Hewlett-Packard, IBM, Microsoft, Novell, Oracle, Siemens, and Sun.

In contrast, *specialty brands* are vendors whose brand names represent specific categories of products. Similar to the way Gap and Banana Republic are clothing brands, IdM vendors with specialty brands closely align their product portfolios with a particular market segment. Specifically, ASG Software Solutions, BMC, and CA are management brands, BEA Systems and Red Hat are platform brands, and Entrust is a security brand. (Note that IBM Tivoli and HP OpenView are also management brands owned by anchor brands.)

Boutiques are vendors that are dependent on the market conditions created by anchor and specialty brands. These vendors typically offer product enhancements and tactical solutions to improve the speed and success rate of IdM deployments. Boutique vendors are represented in Figure 2 in the pink, green, yellow, and blue shaded areas (note that the graphic is not meant to illustrate actual names of boutique vendors).

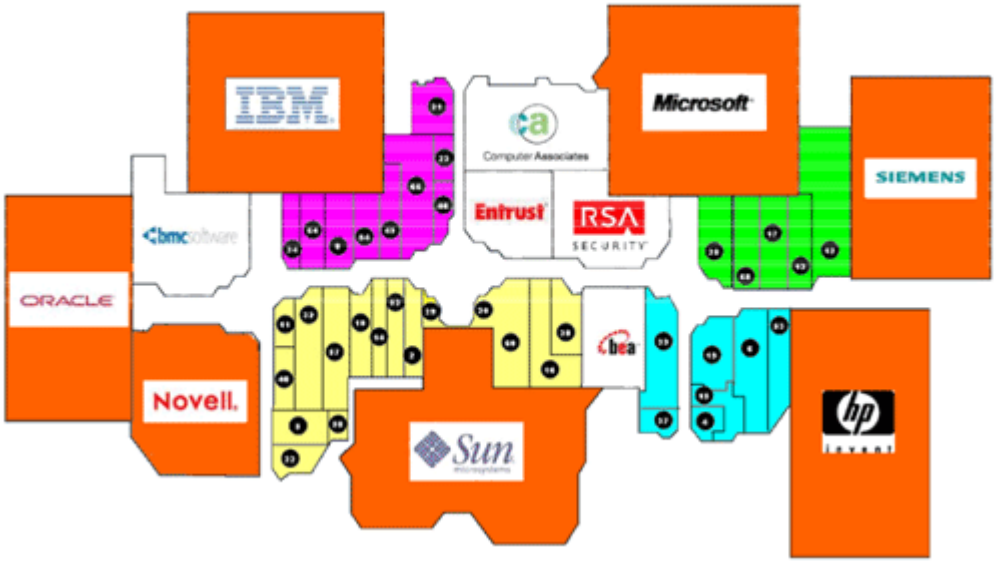

Figure 2: *Anchor, Specialty, and Boutique Brands in the IdM Market*

Despite ongoing merger and acquisition (M&A) activity, the IdM market continues to host more than sixty companies with notable IdM offerings. Table 1 lists many of the vendors in the IdM market.

41st Parameter	Bridgestream	Hewlett-Packard	Persistent Sys.
A10 Networks	CA	IBM	Ping Identity
A-Select	Caymas Systems	IdentiPHI	Prodigen
ActivIdentity	Centrify	Identity Engines	Proginet
Aladdin	Citrix Systems	Imanami	Quest Software
Approva	Cloakware	Imprivata	Radiant Logic
ASG	Consul	Infoblox	Red Hat

Apere	Courion	Jamcracker	SafeStone
Applied Identity	Credentica	Jericho Systems	SAP (Versa)
Approva	Cyber-Ark	Juniper	Secured Services
Arcot	Diamelle	LogicalApp	Securent
Authentify	DigitalPersona	MaXware	Sentillion
Avatier	EMC (RSA)	Microsoft	Siemens
Aveska	Encentuate	M-Tech	Sun
Avencis	Engiweb	nCipher	Symantec
Bayshore	Entegrity	NetIQ	Sxip
Bell ID	Entrust	NetPro	Symlabs
Blackbird	Epok	NeuStar	TNT
BEA	Eurekify	Novell	TriCipher
Beta Systems	Evidian	OMNIKEY	Vaau Consulting
BHOLD	Fischer Intl.	Oracle	Vasco
BioPassword	Forum Systems	OSM	Veridicom
BMC	Gemalto	PassGo	Völcker
BNX Systems	GlobalSign	Passlogix	

Table 1: *Notable Vendors in the IdM Market*

IdM Market Drivers: Security, Regulation, and Cost

The IdM market is experiencing strong growth fueled by acute business, personal, and public needs for security, regulatory compliance, and cost control. Global threats of terrorism, Internet-borne viruses and worms, and identity theft have drawn attention to the fragmented state of security in online systems.

In many cases, security isn't merely voluntary—it's the law. Governments are becoming ever more stringent about regulating online information, and especially information about individuals. Governments worldwide are fueling activity in the IdM market by issuing regulations around the use of identity information in some cases, while requiring better accountability in others. Such regulations oblige organizations to improve their controls over systems and information. As organizations work to upgrade controls over critical infrastructure, IdM is itself becoming part of that critical infrastructure. Software vendors are therefore rushing to include audit, validation, and remediation features in IdM suites.

In addition, historical methods for securing online applications simply are not sustainable from an administrative perspective. The cost of allowing each application to control its own user population and then requiring local administrators to set policies on the use of application resources is problematic in the Internet age. As users access application functionality through web browsers, handheld devices, and intermediary applications, the access and management needs go well beyond the models that existing applications were designed to support. Each application also presents a potential exploitation point for hackers who could wreak havoc on multiple IT systems. Therefore, all enterprise applications require some degree of common security and authorization policy.

In short, for enterprises, the risks of conducting business online are becoming higher, but by current methods, the cost of improving security using current methods is prohibitive. The security costs are also much higher than anticipated, based on prior funding levels at which security was viewed as a control system rather than a business-enabling infrastructure. The focus of IdM vendors, then, is to enable enterprises to increase the security of online systems while reducing administrative cost and improving user satisfaction.

The popularity of IdM is nevertheless always a tenuous condition, because it's largely based on people's heightened awareness of risk. Identity theft in particular has become headline news in major publications. And the relation of identity to controls in corporate governance is of great interest to lawmakers. Accordingly, one goal of IdM technology is to assuage the general uneasiness people feel about the reliability, security, and safety of online computing, especially with regard to a person's reputation and property. In short, the object of IdM technologies is to make the IdM market ultimately less apparent and less noticeable by moving IdM technologies from being “in” to being “inherent.” Identity must become the invisible but invaluable service on the network that makes online services personable, efficient, manageable, and safe, while preserving the interests and privacy of people using the systems.

IdM vendors are generally aware of this dichotomy. It's no mistake that platform vendors, such as Hewlett-Packard, IBM, Microsoft, Novell, Oracle, Red Hat, and Sun, along with management vendors, such as ASG Software Solutions, BMC Software, and CA, are in the market in a big way. Ultimately, the IdM properties they own will become features in their respective platforms and systems management offerings. But before the market can reach that stage of maturity, it requires more of the kind of attention it's now receiving. For large corporations to justify the costs of their investments in IdM, the business case must be much more than strategic. Fortunately, IdM product revenues, both realized and potential, have been providing vendors with the incentives they need to invest in continued R&D of products.

Major Trends in IdM

Current trends in the IdM market evidence a hot market with emergent business models. Vendors continue to remix product features and packaging in search of sustainable, defensible niches. Identity standards are at the threshold of a renaissance that could reinvent identity systems. And the IdM market continues to intersect with other large market spaces, including management, compliance, and online consumer retail systems.

Blending of Management and Identity Management Solutions

Some of the largest IdM vendors are better known for their management brands, namely BMC, CA, Hewlett-Packard, IBM, and Quest (and to some degree Novell). Not surprisingly, these companies have begun blending messages of identity management and IT management. Compliance, audit, and reporting features are moving toward a common framework in the products of these vendors. Their IdM suites are taking on features of ITIL and IT Service Management (ITSM) and interoperating with CMDBs.

For example, BMC populates its CMDB with identity data to enable user-based policies for management processes. Anchor brands Hewlett-Packard and IBM have long placed IdM within their respective management brands, OpenView and Tivoli. Hewlett-Packard plans to integrate the OpenView Service Desk helpdesk solution and Peregrine ServiceCenter with its IdM suite. Hewlett-Packard also plans to link asset provisioning (Peregrine Systems) to its user provisioning system and to provision its CMDB with identity data.

Compliance and Audit

Government regulations have obliged many enterprises to put stronger, more verifiable policies in place. Where these policies are tied to individual accountability, enterprises must tightly link the use of online systems to personal information. Regulations also present a nested problem, in that personal information itself falls under regulatory control, so enterprises must also place controls over the collection, use, and distribution of information in their identity systems.

Vendors continue to tap into the fast-growing market for compliance, auditing, and privacy technologies. As shown in Table 2, many specialty and anchor brands offer the compliance and audit components of an IdM suite. Some of these brands (mostly the management brands) also offer general-purpose audit and compliance products.

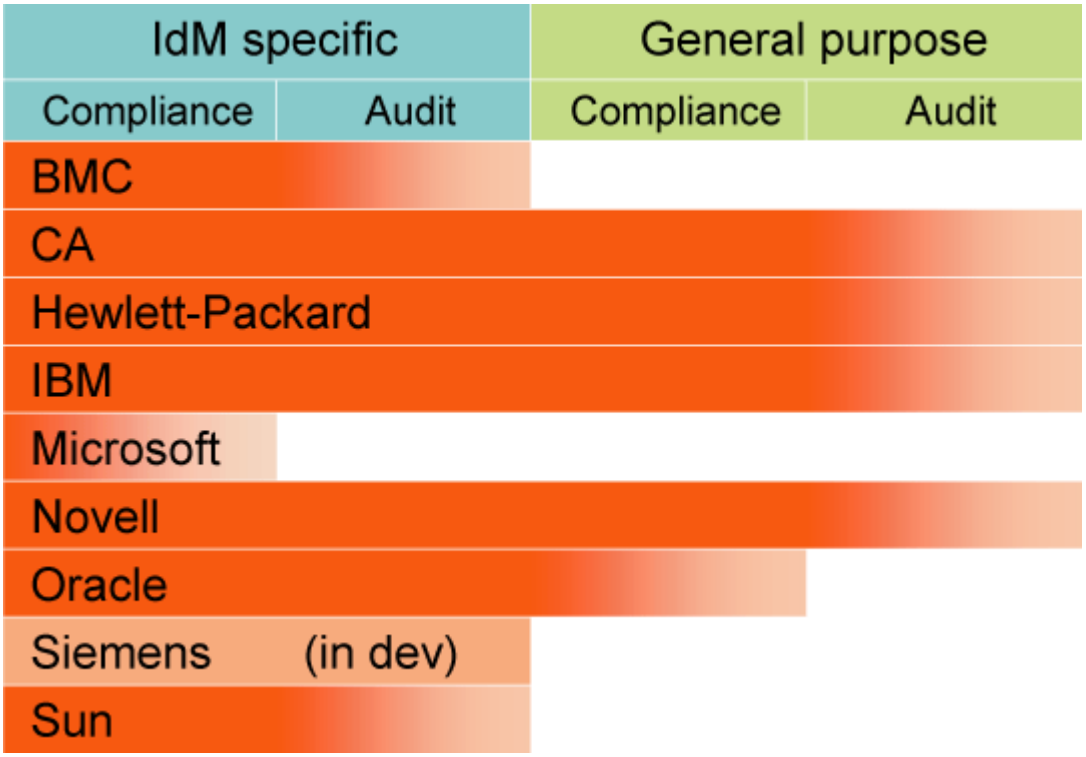

Table 2: *Vendors Offering Audit and Compliance Products for IdM Infrastructure and for General-Purpose Use*

Given the requirements for individual accountability built into regulations such as the Sarbanes-Oxley Act (SOX), general-purpose compliance and audit solutions are increasingly identity enabled. This blending of identity and compliance products will become even more intense over the next few years.

Hewlett-Packard plans to integrate OpenView Compliance Manager, a general-purpose compliance solution, with its IdM suite. The combined solution offers a broad range of features for enterprise-wide compliance, audit, and reporting across an operations infrastructure (including incident response, change management, and asset management) and security infrastructures (security event management, intrusion prevention and detection, and IdM). IBM offers interoperability of its IdM suite with Tivoli Security Compliance Manager, enabling user-based policies for a wide range of compliance solutions.

CA offers several technologies for auditing, alerting, and reporting (including security information management [SIM] and security event monitoring [SEM] products) that the company continues to link with IdM infrastructure. Similarly, Novell acquired e-Security, a security information and event management company, in April 2006, to compliment its existing identity auditing technology. With this technology, Novell intends to build a general-purpose solution for compliance and audit that is strongly identity aware. EMC recently announced its acquisition of Network Intelligence, a SEM vendor. EMC plans to combine the SEM functionality with RSA's security and IdM technology to create a business around information-centric security.

As indicated in Table 2, several other vendors offer products in this converging market. For more information on identity audit and compliance products, see the *Identity and Privacy Strategies* report, "Achieving Organizational Compliance: The Emerging Role of Identity Audit Software."

Consumer Authentication

Largely in response to the rampant spread of identity theft in the United States, the FFIEC (an umbrella entity whose organizations regulate the U.S. banking industry) alerted the industry that it would no longer view passwords as sufficient protection for online transactions. At the time the guidance was issued, existing authentication products rarely reached the consumer market. For example, the authentication products required customers to carry a device with them—which would be both prohibitively expensive for banks and difficult for users. Readers for these devices are also not always available and such devices are still susceptible to man-in-the-middle attacks through phishing or malware.

New solutions are under development to provide a cost-effective but secure alternative to traditional stronger authentication products. One of the early vendors in this space, Passmark, was acquired by RSA, which then, in turn, was recently acquired by EMC. TriCipher also offers products for consumer authentication. For more information, see the *Identity and Privacy Strategies* overview, "Consumer Authentication and the FFIEC Guidance."

Segmentation in the IdM Market

As the number of participants in the IdM market grows, the market is becoming increasingly segmented. Whereas a year ago nearly all IdM vendors sold horizontal IdM solutions to enterprises, today targeted solutions are available for various sectors including government, healthcare, finance, and telecommunications carriers. Many vendors are also beginning to offer IdM products for SMBs. Software vendors frequently partner with integrators and resellers for channel sales and to provide vertical specialization. Regional specialization is also taking hold, with many European companies finding sustainable business in the European Community. Table 3 shows how some of the IdM vendors have approached various market segments. Notably, the financial vertical is already one of the strongest segments for today's IdM products. Nevertheless, vendors are just beginning to create products specifically for the financials vertical, partly in reaction to the FFIEC guidance on Internet banking.

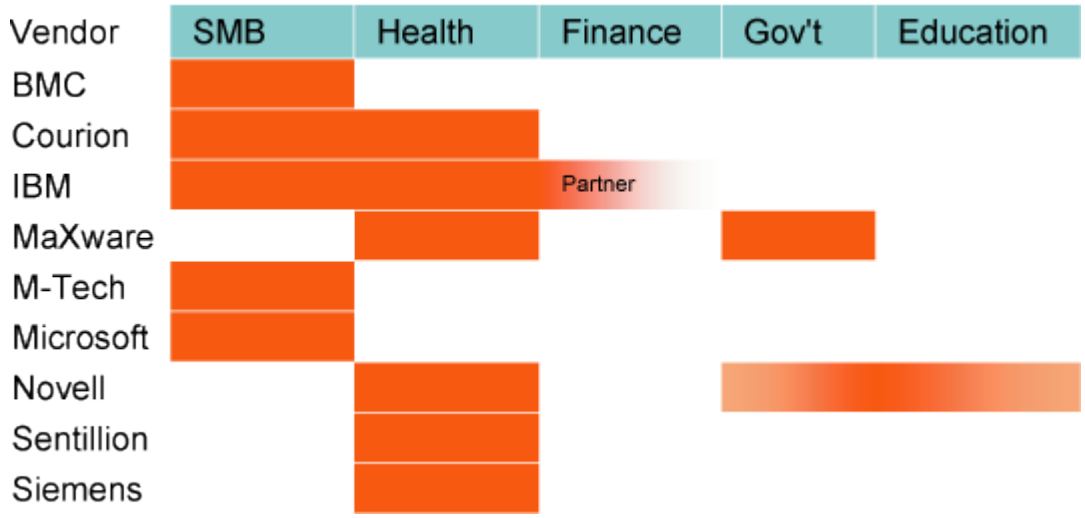

Table 3: *Segmentation in the IdM Market*

IBM in particular has aggressively approached the SMB market. The company already markets to SMBs through its Express brand, and IBM recently certified and packaged its provisioning product to sell through this channel. Dubbed IBM Tivoli Identity Manager Express (TIM Express), the product offers simplified installation and features. IBM followed up that release with IBM Tivoli Federated Identity Manager Lite and Directory Integrator for its SMB channel. BMC also began targeting the SMB market more intensely this year by broadening its support for Microsoft environments. Courion recently released its Jump Start options offering to the mid-market. Rather than creating a separate product offering for the SMB market, Courion ships a scaled down version of their flagship product, which provides customers with a simple upgrade path to the full provisioning suite. Similarly, M-Tech Information Technology continues to see SMBs as a growing aspect of its business.

The healthcare sector has been a hotbed for IdM deployments, and now at least a half dozen vendors offer specific solutions for health care (albeit often through professional services organizations). Sentillion is a boutique provisioning vendor entirely focused on health care. Another boutique vendor, Encentuate, offers SSO and access control for the healthcare and biopharmaceutical industries. Siemens is the largest provider of equipment to health institutions in the United States and therefore has targeted its security and identity products to those organizations. Novell and IBM offer IdM solutions to the healthcare sector through professional services engagements. And Courion and MaXware have garnered a significant amount of their business from the healthcare space and therefore offer features specifically for those customers. EpicTide offers an appliance product for intrusion detection and privacy compliance that specifically targets the healthcare providers.

Role Management and Fine-Grained Access Control

As enterprises tighten control over information systems to meet security and regulatory goals, managing access to applications and data is becoming the core ingredient in compliance solutions. Provisioning products are already benefiting from this emphasis on the now idiomatic “who has access to what” mantra. But managing entitlements at enterprise scale (with potentially hundreds of thousands of workers) at a deeper level than the coarse-grained access control most systems provide is a Herculean undertaking. Several startup vendors have taken on the problem of assigning finer-grained authorization to broad user populations, generally by mapping business roles to access privileges.

Companies such as BHOLD, Blackbird, Bridgestream, Courion, Engiweb, Eurekify, Prodigen, SecurIT, TNT, and Vaau offer various tools for role discovery and management. Many of the anchor brands partner with these vendors to integrate role management with provisioning products. For example, Novell partners with BHOLD, Oracle and IBM partner with Bridgestream.

Frameworks, Tooling, and Standards

IdM is an enabling infrastructure, so without applications that make use of it, the infrastructure loses much of its value. Getting greater application adoption of IdM technologies is therefore a key issue for market progress. As long as IdM and security technologies remain aftermarket add-ons, they will be difficult to deploy and difficult to integrate. The degree to which the IdM infrastructure seeps into application platforms over the next several years will be another factor in how the market plays out. All the major platform vendors now possess IdM technology, and these vendors also claim IdM is crucial to their long-term platform success. Over time, these vendors will instill their platforms with greater IdM functionality.

Security technologies have long been orthogonal to widely used platforms. But security and identity services must be exposed through frameworks that enable division of labor between systems-level programmers, who know how to build secure infrastructure, and business-level developers, who can use declarative techniques to leverage those services in their applications. By analogy, security and IdM technologies are to the network application platform what memory management, scheduling, user interface functionality, and other low-level services were to the stand-alone operating system. Once these features became available as common services in the context of an operating system, more and better applications came to market because developers were able to focus on their areas of expertise. Similarly, when application platforms begin to support application programming interfaces (APIs) that enable developers other than world-class cryptographers to write secure networked applications, a new generation of distributed application will emerge.

The last two years have seen a dramatic shift in the composition of identity standards. Heralding the post-LDAP era of standards building, industry standards groups released an impressive number of progressive standards in a period of about two years, including SAML, Liberty Alliance Identity Federation Framework (ID-FF), WS-Security, WS-Trust, Service Provisioning Markup Language (SPML), and eXtensible Access Control Markup Language (XACML). Although the longevity of some of these standards remains in question (for example, the SAML protocol competes with WS-Trust), together they represent an important inflection point in the design center for identity exchange.

Another shift in identity standards is now on the horizon with the work being formulated around the concept of an identity metasystem. Microsoft has contributed significantly to this effort and plans to release CardSpace, an identity selector based on user-centric principles, with the release of Vista next year. In combination with the Windows Communication Framework, CardSpace offers developers an integrated means of reusing identity and security technologies. Other companies, including Credentica, IBM, NetMesh, Novell, Red Hat, Sxip, and VeriSign, are now contributing to loosely related projects in this space as well. Project Higgins and OSIS are focused on building out user-centric developer models and applications. For more information, see the 2006 Catalyst Conference North America presentations, "Identity Frameworks, Development Tools, and the Emerging Meta System" and "Thinking Outside the Domain: The Emergence of User-Centric Identity and the Trend Toward Pro-Social Management Systems."

Identity Data Services

Burton Group's Reference Architecture Technical Position, "Accessing Identity Data Services," introduces the concept of an identity interface layer, an abstracted, comprehensive interface for exposing identity operations. Until recently, the development of an externalized identity abstraction has been principally an exercise left to IT organizations, requiring custom development with little support from the IdM vendors. Over the next year, vendors such as CA, MaXware, and Oracle will begin releasing tools for constructing identity data services. For more information, see the *Identity and Privacy Strategies* overview, "Enabling Identity Data Services: New Developments in Identity Tooling Provide a Good Start."

User-Centric Identity and the Identity Metasystem

User-centric IdM has long been a topic of academic debate, but over the next year several products and standards will hit the market. Microsoft will deliver CardSpace with the release of Windows Vista, essentially inaugurating the user-centric identity market. CardSpace will be met with industry support from several vendors in the space, such as Sxip and Credentica, who don't have the market-forming ability of Microsoft, as well as from service providers and standards and open source groups. With Microsoft's "open specification promise" announcement, the OSIS project is likely to succeed. Project participants are hoping to deliver something akin to CardSpace in the open source environment. The project has attracted IdM stalwarts, including IBM and Novell, and also companies such as Google, Red Hat, and VeriSign.

The Future of IdM

Today, the majority of IdM infrastructure is software applied to existing, identity-poor online resources. Over time, IdM will permeate the infrastructure by being baked into application platforms, network appliances, development tools, and client operating systems. Standards will make digital identities and entitlements more portable and transferable. As shown in Figure 3, IdM technologies will become increasingly fine grained and enmeshed into the network fabric. Although centers of consolidating identity data and policy will remain—and therefore sustain the market for IdM server products—much of the IdM technology will move onto applications and client devices.

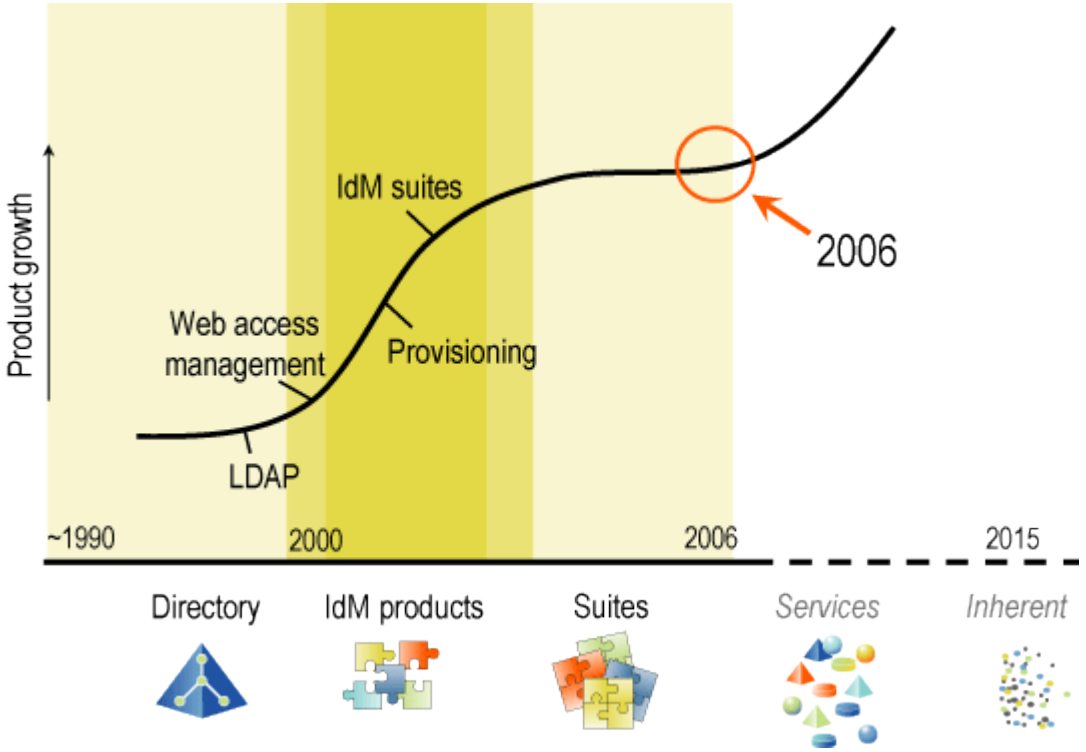

Figure 3: *Progression of IdM Technology*

In some areas, identity features have already seeped into products. The appliance market, in particular, has actively introduced identity features into security and compliance products. Vendors such as A10 Networks, Apere, Applied Identity, Caymas, F5, Identity Engines, Imprivata, Infoblox, and Juniper Networks have led the transition. Products from some of these companies (Apere, Identity Engines, and A10 Networks) are more than just security appliances with identity-aware features. They also offer basic IdM functions and provisioning connectors (Apere even has a connector factory). These vendors are beginning to compete with software IdM solutions, particularly in the user management and provisioning spaces, in both the SMB and the enterprise market segments.

Still, the scale of infusion required to arrive at infrastructure-level IdM is massive and will take time. It will require several releases of operating systems and application servers, followed by new releases of applications that take advantage of IdM APIs. The trend toward integrating IdM in general platform services will prod vendors to break up monolithic suites into service oriented architecture (SOA)-style services. Currently, the economic incentives for doing so aren't sufficiently high. Several anchor brands have only recently acquired IdM technologies and have yet to recover their investments. The market for SOA-based IdM is still emerging, so demand remains low. But given the weight and merit of the business drivers for IdM, progression toward that goal will be relentless until the goal is realized.

Handheld mobile devices continue to evolve toward general-purpose computing devices. Increasingly, such devices will be used for stronger authentication and user-centric control of data. The sheer number of devices on the market will make mobile platforms an extremely important piece of the IdM marketplace.

Internet Identity

It's by now platitudinal that the Internet lacks sufficient infrastructure to guarantee the safety of user populations. Creating such a layer based on digital identity has therefore become an area of intense research and debate. But the Internet doesn't lend itself well to the enterprise-centric technologies that currently permeate the IdM landscape, so architects are looking to new models for promoting social responsibility.

One approach that has garnered noteworthy momentum is user-centric identity. Within the next few years, user-centric technologies will offer users a seat at the bargaining table over how their personal information is used. User-centric technologies won't enable users to have complete control over data flows of their personal information, but the technologies will create value for both the users and enterprise organizations. In particular, an enterprise may find that allowing users more direct control of their information shifts the liability risks of compliance violations away from the enterprise.

Microsoft's upcoming release of CardSpace will have a strong effect on identity in the enterprise and on the Internet. CardSpace will open new possibilities for engaging users in managing their digital identities. And given its uptake outside of Microsoft, the product is likely to meet much greater success than its predecessor, Passport (now Windows Live ID).

But many hazards remain in the path of a user-centric future. For one, orchestrating the ubiquity of such a system is also a task, because in computer networking, the biggest changes generally come from the edge, not the core—that is, from the outside in. In addition, top-down administrative systems don't scale to Internet populations. Therefore, companies traditionally outside the enterprise market, such as Google and Yahoo!, may yet weigh in on digital identity for the Internet.

As user-centric solutions become popular, these tools will impact how enterprises instantiate, and manage, digital ID over the long term. Nevertheless, user-centrism is only one aspect of a polycentric identity system. Every identified subject (person, service, or device) will have some unique view of the Internet world. The science of interconnectivity therefore requires a kind of polycentrism that allows all participants to work within their own contexts and yet interact with the world in a consistent manner.

Given that identity information and the Internet are both CPRs, government regulation always remains a possibility. Where citizens feel a resource is of significant value, but that reliable access to it has become choked with commercial, private, and even hostile interests, governments are likely to step in to police the system. It's not difficult to imagine a time when governments issue surfer licenses in the same way they issue driver licenses today. Governments would then assume the role of identity provider on the Internet.

But other styles exist for promoting civility in a commons. Pro-social styles rely less on issuance of ID cards in favor of connection and relationship to other members of a community. In social style, recognition, reputation, and collaboration have greater weight than the ID card. For more information on social style, see the 2006 Catalyst Conference North America presentation, "Thinking Outside the Domain: The Emergence of User-Centric Identity and the Trend Toward Pro-Social Management Systems," the *Identity and Privacy Strategies* overview, " Thinking Outside the Domain: Revisiting the Function of Identity Information Across Digital Communities," and the *Identity and Privacy Strategies* MBP document, "A Review of Identity Practices in Internet Communities."

Market Impact

The three business models (anchor, specialty, and boutique) introduced in the "Market Participants: A Review of IdM Vendors" section of this report offer enterprise customers slightly different value propositions.

Anchor Brands

Anchor brands have diversified product portfolios (Siemens, for example, offers kitchen appliances and sophisticated medical equipment in addition to its IdM products) and generally bear higher overhead than do the vendors on the other two tiers. Accordingly, these vendors typically offer products in proven markets and leave much of the market experimentation to others. Anchor vendors also rely on volume sales of multiple products to each client, so the pricing models and product suites are arranged to entice clients into strategic purchasing agreements with the brand. With the exception of Microsoft, anchor vendors typically include professional services as a significant component of any sale. Many of these vendors rely heavily on their own application platforms as the basis for their business, and therefore align their products—including IdM suites—toward promoting the platform.

Currently, eight anchor brands have major holdings in the IdM market: EMC (through its acquisition of RSA), Hewlett-Packard, IBM, Microsoft, Novell, Oracle, Siemens, and Sun. Most of these companies achieved a one-stop shopping model for IdM this year. Oracle rounded out its suite this year with acquisitions of Thor Technologies and OctetString, giving the suite strong provisioning and virtual directory technologies. Siemens acquired OKIOK, a WAM vendor, in order to offer WAM functionality natively with its suite. Anchor brands also differ in their support for emerging product categories, such as federation, audit, and privacy solutions.

Although these companies generally compete for the same business, the variations in their business models make each one unique. Enterprises that rely on professional services and prefer to use the same vendor for both product and services will be drawn to IBM and Novell. As the Hewlett-Packard and Oracle consulting practices mature around IdM, the companies will also become well suited for such enterprises. Companies that have a preferred system integrator partner, such as PricewaterhouseCoopers (PwC), Deloitte & Touche, or Accenture, will look to vendors that focus on architecture of deployment and partners for deployment services.

Geography can also play a role, because even though all of these organizations have global presence, a number of factors can make their products more successful in particular regions. Siemens has a large installed IdM customer base in Europe, particularly in the automotive and financial services industries. Novell, IBM, and Sun do well in Europe and in Asia, where they often compete with specialty brands such as BMC and CA.

Several anchor brands rely heavily on a flagship platform for their value proposition. Microsoft is the strongest example, but Oracle and Sun also view their respective platforms as their primary strategic focus in the marketplace. Novell is still in the process of shifting its traditional focus on NetWare to its distribution of Linux, making Novell also committed to the success of its platform. Enterprises committed to a platform provided by one of these vendors may therefore find an affinity to IdM solutions from that same vendor.

Anchor brands have both reacted to and generated much of the hype in the IdM market. These companies entered the IdM market for legitimate business reasons—both strategic and financial. But anchor brands need large markets in order to meet their business objectives, so they also invest in marketing the space, and they do so on a scale that smaller vendors cannot match. In some ways, anchor brands generate interest simply by being in a market; the scale on which these vendors operate—especially when viewed collectively—draws significant attention in international media. They also generate interest through advertising and direct sales. Similar to anchor stores in a shopping mall, anchor brands in the IdM market draw crowds and legitimize the space.

The Role of Specialty Brands

Specialty brands offer IdM products as enablers to their core businesses. Given that each of these vendors is motivated to maximize the association of its brand to a particular function, these IdM offerings tend to inherit the focus of the brand. Unsurprisingly, management brands (ASG, BMC, CA, and Quest Software) offer IdM products as a way to enhance overall IT management. Similarly, Entrust makes IdM a core component of security, and platform vendors such as BEA and Red Hat provide IdM features to enhance the usability and security of their platforms. Citrix Systems is trying a branding exercise involving access, in which IdM also plays a significant role.

Management Brands

ASG, BMC, CA, and Quest offer IdM products as part of their general IT management product lines. Currently, CA has amassed the most IdM technology. BMC began with user provisioning and password management but has since expanded into web SSO by acquiring OpenNetwork. Additionally, BMC has expressed a vision for comprehensive IdM coverage, and so could potentially make other acquisitions in the market. ASG, a longtime player in the mainframe management space, now offers user provisioning and password management solutions. Quest is known primarily for its database and Microsoft management solutions, but with the acquisitions of Aelita Software, Vintela, FastLane Technologies, and Discus Data Solutions, the company is making a play at SSO and IdM management (that is, managing the IdM infrastructure), particularly for Microsoft environments. Figure 4 shows the relative IdM coverage areas of the management vendors.

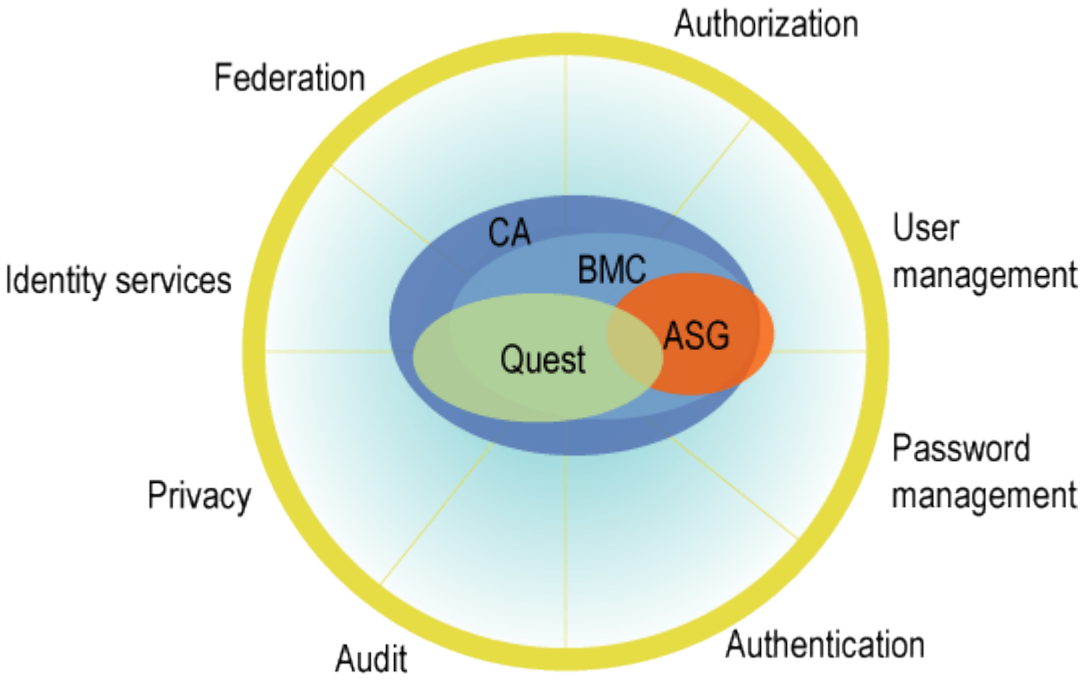

Figure 4: *IdM Feature Coverage of Management Vendors*

Security Brands

Authentication is a key ingredient of IdM, but most vendors defer stronger authentication technology to security vendors, such as Entrust and EMC. Few of the all-in-one IdM vendors offer stronger authentication technologies, and none offer market-leading authentication products. Most WAM products, which include SSO for web applications, provide only simple schemes for authentication, requiring customers to purchase stronger authentication functionality separately from a third-party vendor. Exceptions, of course, are EMC and Entrust, which offer stronger authentication technologies and access management. The strategy for these vendors is to provide IdM products with a heavy security focus.

EMC and Entrust maintain established businesses in stronger authentication and security and so have benefited from IdM market growth. These companies have done reasonably well in extending their concepts of security into other aspects of runtime IdM—namely, web SSO and authorization. But the web SSO segment of the IdM market faces significant price pressure and intense competition, making business growth difficult. Entrust and EMC have therefore turned their interests in IdM to federation and policy-based authorization, which hold the promise of significant growth over the next few years.

Platform Vendors

Because application platforms typically generate an ecosystemic business model, they are usually the domain of anchor brands. Nevertheless, two venerable specialty brands are focusing on platforms: BEA and Red Hat. Interestingly, the business models of these two companies couldn't be more different. BEA sells a proprietary implementation of a Java 2 Platform, Enterprise Edition (J2EE) server, and Red Hat offers an open source distribution of Linux (including an open source application server). And because every platform requires some degree of IdM, both vendors offer some number of IdM features.

BEA acquired CrossLogix in early 2003 and has since offered its web SSO features as part of the BEA WebLogic Server. However, BEA has been relatively inactive in the IdM market beyond that point.

Red Hat is a more recent entrant in the IdM space. The company acquired Netscape's enterprise server technologies, including its directory and certificate server products. These products share a heritage with Sun's current products: The code bases were split between Sun and AOL as part of the iPlanet division. But Sun has since made significant strides with its directory server and has even merged the code with technology acquired from Innosoft International.

All told, Red Hat's present IdM strategy is underwhelming. But what makes Red Hat's moves in the IdM space of greater interest is the company's announcement that it will open source its directory server and possibly other IdM technologies that will be part of its Linux distribution. Still, Red Hat faces formidable competition from other IdM vendors—and in particular Novell—for Linux-based identity services. Figure 5 shows the IdM feature coverage of platform vendors.

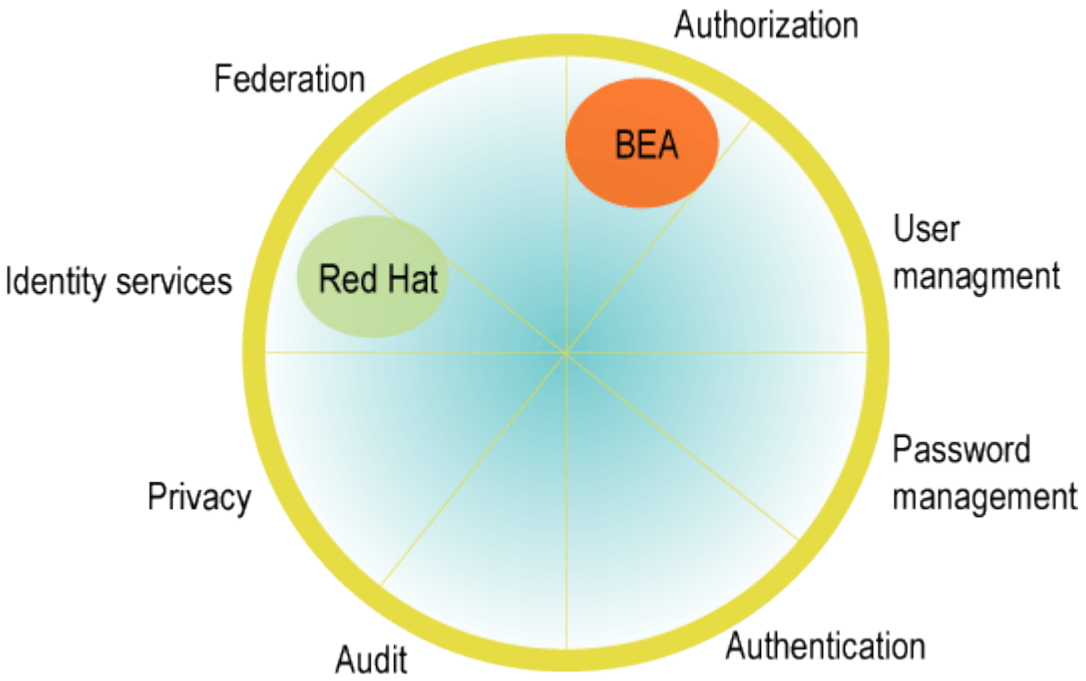

Figure 5: *IdM Feature Coverage of Platform Vendors*

IdM Brands

Several boutiques have grown into self-sustaining, broadly featured specialty brands with a core focus on IdM. This is a new and unsettled area of the market, so the distinction between boutiques and specialty brands in the IdM market is unavoidably tenuous. Evidian operates as an identity brand, but its parent company, Groupe Bull, is a large European anchor brand. Fischer International shifted its focus from e-mail to becoming an identity brand. Courion, MaXware, and M-Tech have emerged as identity brands by diversifying their product portfolios and by maintaining large customer bases.

Evidian has an extensive product line, covering nearly every major aspect of IdM. The company's technology emerged out of deployments at large telecommunications carriers in France and has since made headway in other European countries. Fischer International released an integrated IdM suite consisting of user management, compliance, and identity services functions. The suite is avant-garde, in that it's based entirely on a SOA, offers strong solutions for mobile users, and sports a simple, all-inclusive licensing model. Because the product shipped only a few months ago, it will take time to see how receptive the market will be.

M-Tech Information Technology and Courion, providers of user management products, are becoming identity brands. Courion claims about 300 enterprise accounts and M-Tech about 650, although both companies have more customers using their password synchronization products than their newer provisioning and compliance products.

Figure 6 shows the relative coverage areas of the specialty brands focused exclusively on IdM.

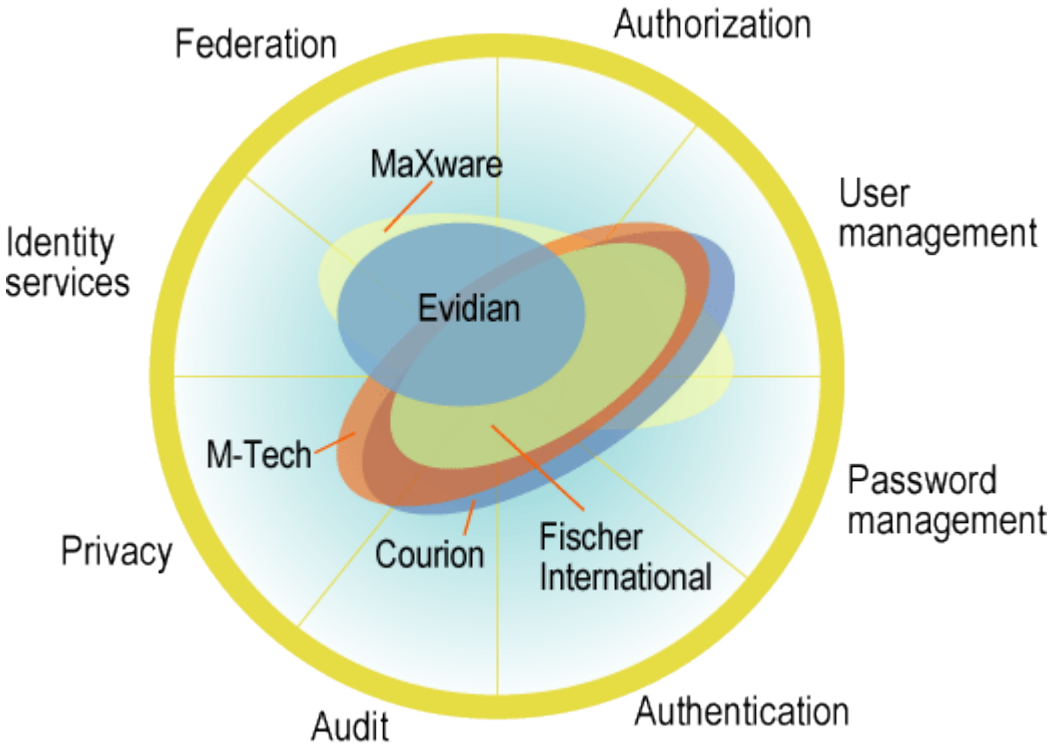

Figure 6: *IdM Feature Coverage of Specialty Brands Focused Exclusively on IdM*

Boutiques in the IdM Market

Several dozen boutique vendors offer targeted solutions in the IdM space. Many of these vendors provide user management functions, such as provisioning, password management, identity services, and ESSO. About a dozen vendors have emerged to create a new space for role management. Ping Identity remains the sole boutique vendor in the federation space.

As boutique vendors, many of these companies have technology partnerships with larger vendors. Figure 7 describes the emphases of notable IdM boutique brands.

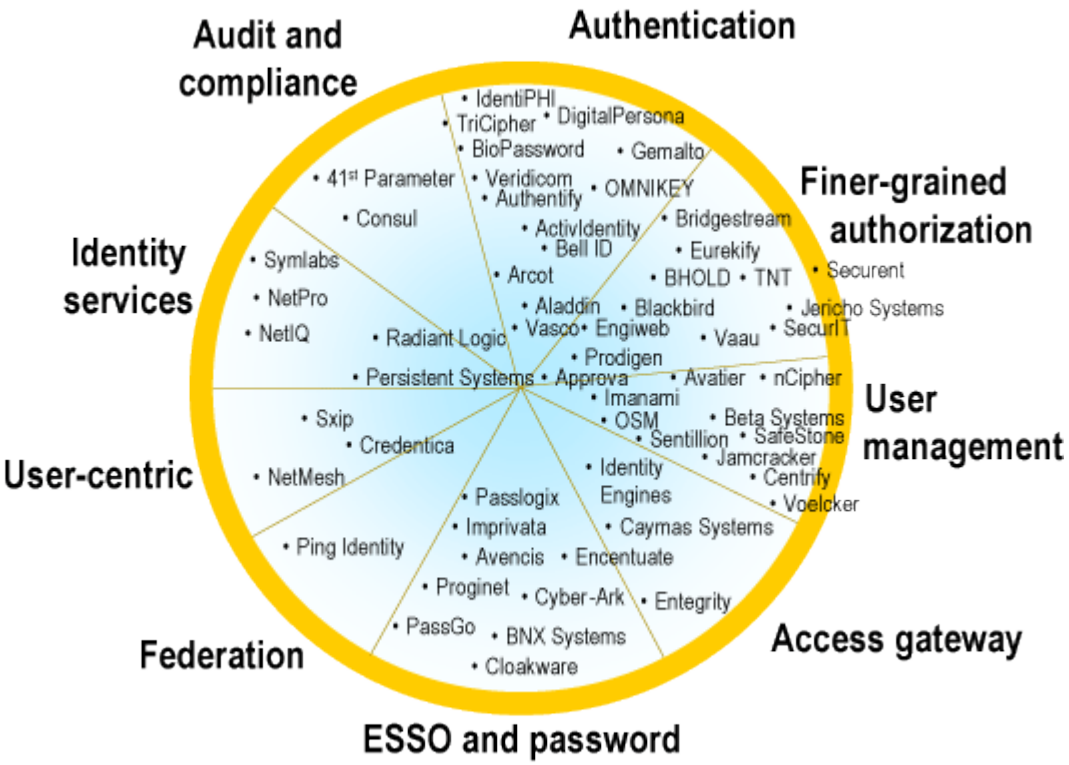

Figure 7: *Boutique Vendors in the IdM Market*

Recommendations

Given the broad scope of enterprise requirements for IdM, prioritizing projects can be very difficult. And with a large number of vendors in this space, product selection also becomes complicated. Combined with the cross-organizational coordination that IdM projects require, the prospects of success often seem daunting.

Nevertheless, organizations that make progress in deploying IdM infrastructure benefit significantly. The most successful organizations are those that approach IdM issues pragmatically—solving important but manageable problems first—while keeping an eye to the strategic goals of the enterprise and staying with a well-documented architecture for IdM. (For more information on creating architecture for IdM, see the *Identity and Privacy Strategies* Reference Architecture.)

Prioritizing IdM Projects

In an attempt to plan for IdM projects, organizations often face questions about whether it's possible to do provisioning without deploying a meta-directory, or whether they can deploy WAM without deploying delegated administration. In general, the question is whether some IdM technologies shortcut the need for others, and so reduce the complexity of IdM deployments.

Such questions are natural, but in a marketplace with several dozen boutique vendors, the answers are often obfuscated. Each vendor has a product to sell and therefore claims that its product requires no (or very few) prerequisites. But IdM products do depend on other components of the infrastructure, which is one of the reasons why larger vendors have corralled stand-alone IdM products into suites. For example, the concept of rule-based access management is simple to understand and, technically, does not require other infrastructure to be deployed. In practice, though, getting dependable input data for evaluating the rules is a very difficult issue that requires identity integration software with meta-directory services, virtual directory services, and provisioning software.

Setting the Project Scope

Setting the scope of an IdM project is not a matter of limiting the technologies or products used in the solution—in fact, mature IdM deployments will use almost all categories of IdM products. Rather, the idea is to define the boundaries of each project, so that it becomes clear what the parameters for success are. For example, a project for "single sign-on" is unbounded. In contrast, a project to create a reduced sign-on environment for five specific applications is likely to succeed, even if it requires that a combination of password synchronization and client-based SSO software must be deployed.

Defining the scope of an IdM project is a matter of graphing three dimensions of the project: the users the project will affect, the type of activities the project will involve, and the applications that will be affected. In defining users, it's usually not sufficient to rely on high-level categorizations such as "employees," "contractors," "partners," and "customers." A more effective definition would be to say the project affects, for example, "the 90 tellers working in the Boston main office and the 100 tellers working in surrounding branch offices." During the planning phase, it's not necessary to actually have a list of users who will be involved in the rollout, but that information will become necessary in the testing and deployment phases.

IdM projects focus on essentially seven types of activities. By differentiating among them and clearly stating which activities a particular project addresses, project managers can create realistic expectations, set product acquisition priorities, and improve the chances for the project's success. Table 4 describes the seven types of IdM activities.

Activity	Description
Account management	Creating, deleting, and removing user accounts; enforcing naming policies on new account creation
Identity synchronization	Ensuring that attributes on an account are accurate and consistent across applications, registries, and repositories
Permission management	Configuring group and role membership and entitlements; setting up data for rules processing
Access management	Runtime enforcement of policy to ensure that users access only resources they're authorized to use
SSO	Enabling sign-on to multiple applications based on a single authentication event, including across federated domains
Credential lifecycle management	Credential issuance, password synchronization, password reset, token provisioning, token expiry and replacement

Advanced federation	Federation scenarios beyond browser-based, inter-site SSO—for example, web services federation

Table 4: *The Seven Activities of Highly Effective IdM Architects*

The activities in Table 4 do not represent a closed canon of IdM functions; they are simply a list of the most common goals of IdM projects. Enterprises may develop their own set of IdM activities, but each activity should be discrete, fully planned, and attainable. Also, these categories don't align with current product packaging. For example, provisioning products offer account management, identity synchronization, and permission management. Many password management solutions provide only synchronization or reset, but not a full set of credential management features.

The third dimension of IdM projects is determining which applications will be affected by the new infrastructure. Although it's possible to roll out IdM infrastructure in an ad hoc fashion, once again, chances of success are much greater if applications involved in a particular project share some commonality. For example, a project may be defined to offer SSO for specific users of Oracle applications or Microsoft products. A project may also focus on applications that a specific group of people uses daily. For example, an IdM project could offer account management and identity synchronization for the ten applications used by sales representatives in North America. Applications may also be enterprise applications that all internal users require, such as e-mail and corporate address books.

Enterprises should then invest in projects based on targeted, yet strategic, goals. These projects should be designed for a particular domain (usually defined by applications, data, and other resources) and by activity.

Get the Fundamentals Right

In any IdM project, certain fundamentals are prerequisite to deploying new applications. These are account reconciliation, identity data integration, and identity repositories. Account reconciliation involves identifying and linking accounts in various repositories that represent a single individual. In some cases, sufficient data exists in each repository to create a link automatically. But a large number of accounts cannot be linked through join logic alone. For these cases, enterprises require tools to identify accounts, solicit the help of users to provide additional information, and verify proper linking by administrators. Courion, MaXware, M-Tech, Oracle, and Sun offer technologies to facilitate the account reconciliation process.

The next step is to ensure that the IdM solution has accurate identity information to draw upon. Where distributed identity data must be consistent, meta-directory products can synchronize information continuously. In cases where there are multiple authoritative sources of identity information, or where privacy, security, or performance requirements make synchronization unfeasible, virtual directory services can enable identity integration. In some cases, federating identity between multiple, internally integrated business units may be a better approach than attempting wholesale consolidation and integration of identity across business units. Increasingly, federated identity will become the preferred choice for intra- and inter-enterprise applications.

As IT departments budget for identity services, they should work to create balance in the types of projects they take on. Companies with urgent needs for compliance and federation solutions may overinvest in infrastructure that presumes a stronger identity foundation. Figure 8 arranges IdM activities in a pyramid to show a rough approximation of the relative investment that IT departments should give to various IdM activities.

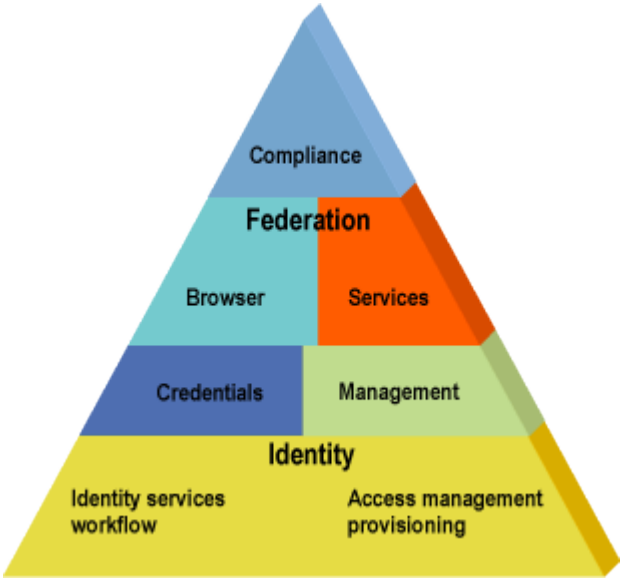

Figure 8: *IdM Project Investment Pyramid*

Anchor, Specialty Brand, or Both?

Most IT organizations want to rely on a primary provider for the bulk of their IdM infrastructure. Boutique vendors usually don't provide the necessary scope to be the primary IdM provider for an enterprise. This leaves enterprises with a choice between anchor brands and specialty brands. Enterprises can then bring in boutique vendors as needed to fill critical pieces in the IdM architecture.

Because many anchor brands also control application platforms, much of the technology they produce improves the manageability of the native platforms. It's likely that some aspect of an anchor brand's IdM functionality will be required in using that vendor's platform and applications. For example, enterprises deploying Windows Server will require Active Directory. So, using IdM technology from an anchor brand is the inevitable outcome of using the vendor's other products. Nevertheless, IT departments will also need general-purpose, cross-platform IdM solutions and, for this role, specialty vendors often have the advantage.

In most cases, deploying IdM infrastructure will require integration across brands—that is, across IdM suites—to get sufficient coverage of an enterprise's identity resources and to set up connections with external partners. Part of the evaluation of which products to use will be based on the technical merits of candidate products. The brand an organization prefers in purchasing enterprise software is largely a matter of principle. For example, organizations take many brand-oriented variables into account, such as single vendor versus best of breed, outsourcing versus ownership, and the degree of vendor risk (for more information, see the Reference Architecture Principles.) Customers debate the merits of each approach in the IdM space; but often, determining the best approach requires the context of the business model.

Vendor Selection

In focusing product acquisition on the four primary categories of IdM (authentication, authorization, user management, and validation), an enterprise can then choose to purchase multiple categories from a single vendor or to consider each category as a separate purchasing decision. Few vendors have product coverage across all four areas. For example, Microsoft, EMC, and Entrust offer advanced authentication products that include public key infrastructure (PKI), and Entrust and EMC offer additional authentication methods (including tokens, biometrics, and mobile devices). However, each relies on technology partners to supply other pieces of its IdM strategy. VeriSign provides user management, authorization, and advanced authentication—but only through managed services. Other vendors offer authorization and user management products, but do not sell advanced authentication products.

Given the diversity of large organized networks, enterprises may find the need to purchase multiple products from multiple vendors in each category. For example, an enterprise may choose to purchase multiple authentication products. However, within each category, enterprises should look for products that are multifunctional and versatile. When acquiring provisioning technology, for example, customers should demand bidirectional synchronization and meta-directory features as well. SSO functionality may also be useful in this category, because it can accelerate IdM rollout to applications that have not been modified to natively use IdM features. Enterprises might also elect to purchase a niche product—such as a virtual directory service or federation toolkit—to satisfy a thorny application, data, or partner integration problem.

The Details

More than 90 vendors offer products in the identity management (IdM) market. Because these vendors all sell multifeatured IdM products, they defy simple subclassification. This report segments vendors based on a brand's business model. Anchor brands are companies with diversified product portfolios, so that the brand is not associated with any particular market segment. Specialty brands are multiproduct companies with a focus on a particular market niche, such as security, management, application integration, or identity. Boutique brands are companies that offer a single product or a small number of products in a very targeted market segment and rely on anchor and specialty brands to drive the market.

Anchor Brands

The IdM market enjoys the support of the world's leading technology companies, including EMC, Hewlett-Packard, IBM, Microsoft, Novell, Oracle, Siemens, and Sun Microsystems. These vendors have invested heavily in the space, largely through acquisition of early entrants into the market. Each of these vendors now boasts IdM suite functionality.

EMC/RSA Security

Before 2006, EMC was known largely for its backup and storage solutions; the company also offered several virtualization solutions, including VMware. But in 2006, EMC acquired Authentica, a digital rights management (DRM) vendor, RSA, an authentication and IdM vendor, and Network Intelligence, a security event monitoring (SEM) vendor. The company now plans to combine its newly acquired technologies to deliver "information-centric security." EMC says the company will market its information-centric security solutions under the RSA brand. EMC inherits the following IdM-related products from its acquisitions:

- RSA Access Manager (a web access management [WAM] product)
- RSA Sign-On Manager (an enterprise single sign-on [ESSO] product)
- RSA Federated Identity Manager (a stand-alone federation server)
- RSA Reporting & Compliance Manager (as the name suggests, a compliance tool)
- RSA Authentication Manager and RSA SecurID (stronger authentication products)
- RSA SecurID smart cards and card management system
- RSA Digital Certificate Solution line
- RSA BSAFE (a developer toolkit and key management system)

Hewlett-Packard

Although Hewlett-Packard has dabbled with IdM technologies before, it began a serious venture into IdM in 2003 with the purchase of the Select Access technology from Baltimore Technologies. Hewlett-Packard went on to announce that it will acquire TruLogica, a provisioning vendor. Hewlett-Packard has since developed audit and compliance products that leverage its IdM suite.

As a vendor with a large, worldwide presence, Hewlett-Packard can compete with any of the current IdM players. Hewlett-Packard purchased companies with strong technology but insufficient market presence—something Hewlett-Packard can easily rectify. But although the technology appears strong, Hewlett-Packard has struggled to challenge other anchor brands' share of the market. It currently claims more than 150 direct customers of its IdM products (not including shipments of bundled products), which is an impressive number for a comparatively recent entrance to the market. However, several of its competitors already boast customers in the thousands.

Although Hewlett-Packard is also a platform vendor (of HP-UX and NonStop), the company's IdM solutions show no sign of favoritism for in-house platforms. As part of the OpenView product division—a management brand—Hewlett-Packard's IdM portfolio takes on the flavor of a specialty brand hosted by an anchor brand. That portfolio currently contains three products:

- HP OpenView Select Identity (a user provisioning solution)
- HP OpenView Select Access (a web single sign-on [SSO] solution)
- HP OpenView Select Audit (an auditing and compliance tool for the IdM suite)
- HP OpenView Select Federation (a stand-alone federation server)

IBM

IBM entered the IdM market aggressively by acquiring several companies to form a comprehensive IdM suite. IBM now claims that over 1,700 customers are licensed to use its IdM suite. IBM is frequently mentioned by competitors as the “one to beat” for IdM business.

Currently, IBM's product line includes:

- IBM Tivoli Identity Manager
- IBM Tivoli Identity Manager Express (TIM Express)
- IBM Tivoli Access Manager for e-business
- IBM Tivoli Access Manager for Operating Systems
- IBM Tivoli Access Manager for Business Integration
- IBM Tivoli Access Manager for Enterprise Single Sign-On
- IBM Tivoli Federated Identity Manager
- IBM Tivoli Directory Integrator
- IBM Tivoli Directory Server

IBM has significant resources for research and development (R&D) and has demonstrated a willingness to both build and buy technology. As a result, IBM remains a vendor with great breadth of technology. It also brings a significant in-house professional services organization to bear, both for functional and business processes support. And although IBM sometimes hesitates on various specifications efforts (in particular, Liberty Alliance), in the end, the company has proven a willingness to be both customer and business driven. IBM currently supports and combines Security Assertion Markup Language (SAML), Liberty Alliance, and WS-Federation with provisioning and web services security.

Microsoft

Microsoft was one of the first anchor brands to invest in IdM, through both acquisition and development. Active Directory (AD) is now in use at nearly every enterprise organization. However, AD hasn't displaced other directory services. Additionally, Microsoft's IdM solutions based on AD have been slow in coming and so haven't competed well with other IdM components, such as WAM and password management. Its meta-directory and provisioning solution, Microsoft Identity Integration Server (MIIS), has fared reasonably well, however. Microsoft's recent work on federation and certificate services will likely attract widespread use. Microsoft currently offers the following products:

- Windows Server AD:
  - AD Domain Services
  - AD Lightweight Directory Services
  - AD Certificate Services
  - AD Federation Services
  - AD Metadirectory Services

- MIIS 2003, Enterprise Edition

Microsoft will release user-centric identity features in Vista called CardSpace. Given the support for this concept in the open source community, the technology is likely to create a new category in the market next year.

Microsoft fostered a small community of boutique vendors that extended the reach of MIIS and AD beyond traditional Microsoft borders. Though a reasonable approach, it has not proven to be sustainable. A number of these vendors—namely Blockade Systems, Oblix, and OpenNetwork—were acquired by organizations less committed to Microsoft's strategy. OpenNetwork was acquired by BMC Software; BMC and Microsoft have now begun to sell jointly. Another Microsoft partner, Vintela, was acquired by Quest Software; but fortunately for Microsoft, Quest Software is making a move to be a pre-eminent provider of Microsoft-centered IdM. Other vendors remain less enthusiastic about opportunities with Microsoft.

Novell

Novell has been building out its IdM suite since the mid-1990's and currently offers integrated products for directory services, access management, provisioning, meta-directory services, password synchronization, web and enterprise single sign-on, user management, SIEM, and auditing. The products amount to more than $300 million in annual license revenues for the company. Novell offers strong directory and provisioning services and is expanding into audit and compliance products. It also offers federation services integrated with Novell Access Manager.

Novell's IdM product line includes the following products and solutions:

- Novell Identity Manager
- Novell eDirectory
- Novell Integration Manager (integration development kit)
- Novell iChain/Access Manager (WAM and federation)
- Novell SecureLogin (ESSO)
- Novell Audit
- Sentinel (acquired with e-Security, to be rebranded)

After the acquisition of SUSE and integration with its NetWare base, Novell became a major Linux distributor, but its IdM products remain cross-platform. Novell also offers some of the most compelling integration of identity services with other aspects of its portfolio, including its platforms, systems management, messaging, and security solutions.

Oracle

Oracle sprang into the general-purpose IdM arena with rapid-fire acquisitions of Phaos Technology, a federation toolkit vendor, Oblix, a WAM vendor, Thor Technologies, a provisioning vendor, and OctetString, a virtual directory vendor. Oracle has used these components to build broad security features into its Fusion Middleware platform and continues to expand into audit and compliance. Given Oracle's significant investment in the last few years, Oracle now has tremendous momentum in the IdM market. For more information, see the *Identity and Privacy Strategies* report, "Oracle's Approach to Identity Management: Integrate with Business Applications," and the *Identity and Privacy Strategies* Product Profile document, "Oracle Xellerate Identity Provisioning."

Oracle has moved quickly with the rebranding effort of its newly acquired technologies under the Identity Management 10*g* R3 release. The product line now includes:

- Oracle Access Manager
- Oracle Identity Manager
- Oracle Identity Federation
- Oracle Internet Directory

- Oracle Virtual Directory
- Enterprise Single Sign-On Suite
- Oracle Web Services Manager

Siemens

Siemens is a longtime player in the IdM market, having released its directory server product back in 1991. The company went on to deliver meta-directory services and provisioning products. Siemens has significant market presence in Europe, where the IdM solutions were originally marketed. The company also enjoys a strong partnership with SAP and Siemens now provides integration of DirX Identity with SAP systems—again making it a European preference. In October 2006, Siemens' identity products officially became part of Siemens Medical Solutions. The company plans to deliver identity solutions to the healthcare market while selling to other industries through channel partners.

Siemens' product line currently includes:

- DirX Identity (an IdM suite that includes provisioning and WAM)
- DirX Access
- DirX (a directory server)
- DirX Extranet Edition (a highly scalable version of DirX)

Sun Microsystems

IdM is a core driver for Sun's success in the enterprise software market, and Sun has aligned its business plans in support of its IdM group. The IdM division is now a separate business unit with its own profit and loss metrics.

Sun capitalized on its acquisition of Waveset Technologies (which Sun paid dearly for, in comparison with other provisioning vendor acquisitions) by turning its flailing directory-centric IdM business into an extensive IdM suite. Since the acquisition, Sun has also added an audit and compliance product, so Sun now covers all four of the major components of IdM, and it continues to improve its identity synchronization and virtualization technology. Currently, Sun offers the following IdM products:

- Sun Java System Identity Manager
- Sun Java System Identity Auditor
- Sun Java System Access Manager
- Sun Java System Directory Server Enterprise Edition

Specialty Brands

Several specialty brands offer IdM suites, including ASG Software Solutions, BMC Software, CA, Courion, Entrust, Evidian, M-Tech Information Technology, MaXware, and Quest Software. For information on M-Tech and MaXware, see the *Identity and Privacy Strategies* Product Profile documents, "M-Tech IDM Suite 4.0" and "MaXware Identity Center."

ASG Software Solutions

ASG provides a wide array of management software for enterprise information technology (IT) organizations. The company, which specializes in mainframe computing, has made over 30 acquisitions in its history and now employs over 900 people. ASG's security solutions include the following IdM products:

- ASG-Entact ID
- ASG-Focal Point

- ASG-Global Trust
- ASG-Admin for Security Server
- ASG-Audit

BMC Software

BMC Software is a $1.3 billion worldwide software vendor focused on enterprise management solutions. With regard to IdM, BMC is taking a multifunctional product approach and now claims over 800 customers use its IdM solutions. A distinguishing factor in BMC's solution is its high degree of connectivity to mainframe and UNIX systems, but the company offers a wide range of operating systems.

BMC Software has increased its coverage in the IdM market by acquiring Calendra and OpenNetwork. With technology from these companies, BMC added WAM, directory management, and virtual directory services to its IdM feature list. In addition, BMC has formed partnerships with Consul and Passlogix for risk management and ESSO, respectively. BMC Software has continued in the commitment OpenNetwork had to the Microsoft platform. BMC Identity Management for .Net is designed specifically to leverage MIIS and Active Directory features. BMC has also expanded its offering by adding Compliance Manager and a Directory Application development environment.The BMC Identity Management product family currently includes:

- BMC Identity Management Suite
- BMC Identity Management for .NET
- BMC Identity Directory Management Studio
- BMC Identity Federation Manager
- BMC Identity Compliance Manager
- InSight Security Manager for BMC Identity Management by Consul
- v-GO Single Sign-On (SSO) for BMC Identity Management by Passlogix
- v-GO Self Service Password Reset (SSPR) for BMC Identity Management by Passlogix

CA

In the last five years, CA has gone from having very few IdM products to having an overabundance of products. The company has both engineered its own solutions and acquired companies. In support of its identity and security product lines, CA acquired two products—Cleanup for ACF2 and Top Secret Security—from Infosec. CA also pulled off the largest acquisition in the IdM market to date with its acquisition of Netegrity. CA has since been working to merge the code bases of its existing products, which had significant overlap with those of Netegrity. CA's and Netegrity's customer lists didn't have nearly as much overlap, however, and the combined company now claims more than 5,000 IdM customers.

Currently, CA's IdM suite consists of the following products:

- CA Identity Manager (identity administration, provisioning, and password management)
- *e*Trust SiteMinder (WAM and browser federation)
- *e*Trust SiteMinder Federation
- *e*Trust TransactionMinder (web services security)
- *e*Trust SSO (ESSO)
- *e*Trust Directory
- *e*Trust ACF2 and *e*Trust Top Secret, Cleanup, and Examine
- *e*Trust Access Control (UNIX, Linux, and Windows access control for system administrators)
- *e*Trust IAM Toolkit (fine-grained authorization for applications)
- *e*Trust Security Command Center (a security information management [SIM] product for security auditing, monitoring, and reporting; not included with the IdM suite)

Courion

Courion is a Massachusetts-based company founded in 1996. Courion's first product offering was PasswordCourier, a self-service password management solution. Over the past 10 years, the company has expanded its IdM product line. Today, the Enterprise Provisioning Suite includes:

- AccountCourier
- ComplianceCourier
- RoleCourier
- PasswordCourier
- ProfileCourier
- CertificateCourier

Courion has a respectable share of the IdM market, with more than 300 customers who have (according to Courion) deployed some portion of the Enterprise Provisioning Suite to more than 6 million users. To stay competitive against larger IdM suite vendors, Courion must continue to develop technologies that improve the ease of use of the system and continue to build strategic partnerships to extend the capabilities of its solution. For more information, see the *Identity and Privacy Strategies* Product Profile document, "Courion Enterprise Provisioning Suite."

Entrust

Entrust is now focused on delivering authentication and authorization technologies for web-based, client-server, and web services applications. Entrust's product line includes Entrust GetAccess (a WAM product), Entrust TruePass, Entrust Entelligence, Entrust Secure Transaction Platform, and Entrust Certificate Services for authentication and authorization. The company has also formed reseller partnerships with Sun, Passlogix, and Rainbow Technologies; these partnerships enable Entrust to show the customer a single storefront for extensive IdM solutions.

Entrust now claims over 200 customers of GetAccess. Entrust also serves over 1,000 customers of its authentication products. The company has been active in forming and supporting IdM standards.

Evidian

Evidian is a wholly owned subsidiary of Groupe Bull, a $1.5 billion IT firm with a global presence. Evidian offers a platform-neutral IdM software suite, covering both web and legacy environments. The company recently consolidated its products into AccessMaster, an IdM suite with nine independent, integrated modules. The suite includes the following modules:

- Identity Manager
- Provisioning Manager
- Certificate Manager
- Approval Workflow
- Secure Access Manager Standard Edition
- Secure Access Manager Web Edition
- Secure Access Manager J2EE
- SSO Xpress Standard Edition
- SSO Xpress Web Edition

Unlike vendors with comparable IdM coverage, Evidian built all its IdM products internally, and therefore offers tighter integration among product components. Evidian claims more than 160 customers of its IdM products, most of whom are located in Europe and Asia.

Quest Software

Quest Software has offered tools for Active Directory management and migration for many years. Last year, Quest acquired Vintela, a company that provided Active Directory features—including login—to UNIX and Linux environments. The move makes Quest Software a vendor both for runtime and background management of identity. Currently, the IdM product line includes:

- Management Suite for Active Directory
- Migration Suite for Active Directory
- Vintela Authentication Services

Conclusion

The identity management (IdM) market is a fast-growing space focused on some of today's most pressing technology issues: digital identity, privacy, security, authorization, and account management. The criticality of identity technologies is not lost on the world's largest software vendors, most of which now have IdM strategies and products in hand. Given the nature of the market, vendors will find it difficult to dominate the space, and so many areas of IdM will remain hotly contested in 2007. During this period, enterprises must forge ahead with IdM projects to better secure online resources, comply with regulations, and reduce operational costs.

Author Bio

Mike Neuenschwander

Vice President and Research Director

Emphasis: Identity management, federation, directory services, meta-directories, access management, privacy and regulatory compliance

Background: Has 12 years of network industry experience as a writer, product designer, product manager, and industry analyst. Prior to his work at Burton Group, Mike initiated projects for NDS 8 eDirectory, Identity Manager, and ZENworks at Novell, Inc. Wrote user manuals and helped design network administration products for Intel's LANDesk product line.

Primary Distinctions: Received the Novell President's Award for 1999 and an Novell Employee of the Year Award in 1998. Pioneered the use of XML and middleware in directories.