COMPETITIVE ANALYSIS SERIES

Identity Management
September 2007

Table of Contents

Introduction

In today's global economy, people interact with one another more than ever before. The advances in – and tremendous growth of – Internet technology, along with the worldwide availability of networked communications and multiple access devices have created the need for ongoing access at any time, any place and from any appliance.

Internet-based business processes and a collaborative framework – whether they are global meetings or transactional purchases from a business on the other end of the globe – all require trust. There is a need to build trusted environments where the identity of each user can be established before access rights are granted. These must be trusted environments where customers can gain on-request access to personal and account information without running the risk of falling prey to identity theft. Employees want unencumbered access to corporate networks, systems and applications irrespective of their location. And business partners and suppliers need to be provided with certified access channels to collaborative information sources.

The scope and requirements needed to manage user identities have greatly evolved in recent years. Users make requests. They pay for goods and services. They work in disparate locations. They add to growing information silos. And they do this with 24/7 real time access.

Organisations can no longer use simple authentication tools like passwords. With increasing security risks and growing compliance regulations, this simply cannot be the mode of operations.

Identity management (IdM) technologies have become a key priority for many companies. By deploying identity management, organisations lay the foundations for building a trusted environment between their users and the corporate or commercial systems they're accessing. They also wish to gain efficiency and cost reductions in their operational processes, along with improved productivity from real time access to resources whenever they're needed. They also seek a greatly enhanced ability to prove regulatory compliance by being able to audit who accessed what and when and what they did with the information. The main technologies used include provisioning, single sign-on, access control and authentication.

This analysis examines how identity management vendors are positioning themselves in the global identity management market as well as the issues surrounding the issues driving companies to consider identity management solutions in the first place. This report will also review their strategies and the future directions the providers expect to take.

Identity management: The business issues

Today's companies are presented with tremendous new growth opportunities . . . and competitive pressures. They must be able to generate new revenue lines and acquire new customers through the rapid delivery of new services. Plus, they have to make certain that their current customers are content and remain loyal by enhancing their existing product or service offerings and providing the best possible customer experience. Financial services, banking, retail and even government are among the verticals that have launched new ranges of cost-effective, self-service business channels. However, this multiple systems access from any place at any time has driven the need for risk mitigation, security and compliance to be paramount. However, many companies are poorly placed to deal with these challenges.

"UK companies are poorly placed to deal with identity theft; only one percent has a comprehensive approach for identity management, i.e., authentication, access control and user provisioning. 84% say there is no business requirement to improve this." – UK Department of Trade and Industry Information Security Breaches Survey of 2006

Risk, security and compliance

Identity management is a security issue which is becoming increasingly challenging as the boundary of the organisational network deteriorates. This was well illustrated by the UK Department of Trade and Industry (DTI) Information Security Breaches Survey (ISBS) of 2006. This study reported that one in five larger businesses had a security breach associated with weaknesses in their identity management.

Risk mitigation is a clear driver of security-related policies. An organisation may implement certain policies to achieve more comfortable levels of risk. For example, a company with no regulatory or standards-based requirements for two factor authentication may still choose to implement a solution to minimise risk associated to a given application.

Without identity management, organisations have security weaknesses that intruders or rogue staff can exploit. Compliance demands continue to drive security and risk management priorities. So these initiatives occupy center stage in IT and security projects, with multiple government and industry regulations behind the many of today's identity management projects. From Sarbanes-Oxley and the Data Protection Act to HIPAA and Visa Account Information Security Standards, the common denominator of these regulations' security and privacy components is establishing proper authentication practices and appropriate assignment of privileges. Developing, enforcing, and auditing authentication and access control policies are core elements of compliance projects.

"Many large businesses struggle to set up new users with the right access on a timely basis. Revoking access rights when staff leave or change roles is also a challenge." – UK Department of Trade and Industry Information Security Breaches Survey of 2006: Identity and Access Management

Therefore, without identity management, companies can't have solid audit trails of who did what and when. As a result, compliance procedures are inevitably weak. Effective identity management solutions do this by delivering tools and processes to increase security and trust, facilitate compliance and control costs.

Identity management: The technology issues

Identity management has essentially taken on the role of technology police. There are multiple authentication methods and tools available to kick start the front-end identity management process, including:

- Biometrics
- Identity cards
- IP Security (IPSec)
- Passwords
- Public Key Infrastructure (PKI) digital certificates
- Secure Sockets Layer (SSL)
- Smartcards
- Tokens
- USB devices
- Virtual Private Networks (VPN)

However, many organisations still don't operate with standard sets of systems and platforms, nor do their existing infrastructures possess consistent integration and interoperability capabilities. In many instances, their current platforms, systems and networks already experience problems being able to "talk to one another." As a result, identity management becomes more difficult.

UK businesses still overwhelmingly depend on user IDs and passwords to check the identity of users attempting to access their systems. Many large UK businesses have also reported that they believe there is no business requirement to move to stronger forms of authentication. Others cite cost, user inconvenience and implementation or deployment issues as major barriers (see Table 1). However, for companies that have seen unauthorised staff access are more likely to invoke stronger authentication methods.

Table 1. Reasons that large UK businesses with weak authentication do not implement stronger authentication

Reasons	Percentage
No business requirement	60
Cost	29
User inconvenience	19
Implementation or deployment issues	13

Source: UK DTI ISBS 2006

When organisations first determine which users can have access to their systems and applications, they utilise core elements of the IdM technology – like single sign-on (SSO) and two-factor authentication – to ensure that control and access services are put into motion.

However, while SSO is often viewed as a component that delivers security and business efficiency, there doesn't appear to be a minimum service standard. Butler Group reported that, in their belief, SSO is delivered with a lax supporting security model: either inappropriately factored authentication or password-centric solutions only too happy to cater to corporate malcontents.

Two-factor authentication has been viewed as an identity management holy grail of sorts. It provides strong access controls, but the Butler Group feels that little has been done to ensure that each factor of the authentication model adds value in terms of the extra security layer it's said to provide.

Organisations need a clearer, more focused technology delivery model. It should be easily understood by the companies using it as well as one that supports the delivery of solid end user benefits.

Identity management trends

"Compliance has changed the landscape; it has changed enterprise identity management."

In his keynote presentation at the recent 2007 Digital ID World conference, Burton (analyst) Group CEO Jamie Lewis said that compliance issues are now changing the focus of identity management. Lewis said, "Compliance has changed the landscape; it has changed enterprise identity management."

It is Lewis' belief that identity management has not yet mastered issues such as password synchronisation, single sign-on, provisioning and privileges, but the technology has become more aligned with supporting access control, management, verification and authorisation. While the foundation of identity management involves business processes and a supporting infrastructure, the current trends suggest that users are focused on using those foundational elements for identity-based access control to systems and resources based on company policies. In a nutshell, Lewis says that users are now locking down access and are logging and auditing who is using their systems and when and what data they are accessing.

"Three quarters of financial services companies believe compliance with laws and regulations is a very important driver for their security expenditure." – UK Department of Trade and Industry Information Security Breaches Survey of 2006: Identity and Access Management

In addition, Lewis believes that the trend has fueled the development of identity-based risk management, auditing, and policy enforcement tools from several vendors. The trend has also led to a slowdown in the development of identity technology, which some users say is not living up to original expectations, particularly around federation. Compliance has contributed to the slowdown, as have new user-centric identity models, which have led to questions about where the true value lies in identity projects.

According to Forrester's Jonathan Penn, the primary driver for enterprise investment in identity management will shift from compliance to security and, specifically, to information protection. Compliance will continue to strongly influence market direction, but vendors will focus on new areas, such as physical-logical security convergence projects like ID cards and restricting privileged user rights. Penn believes that users will invest in provisioning, enterprise single sign-on (ESSO), and strong authentication technologies. Additionally, biometrics, federation, risk-based authorisation and enterprise application security integration (EASI) tools will start to command attention beyond the security early adopter market.

The identity management software marketplace

Identity management vendors are currently expanding the footprint of their offerings through internal development, partnership, or acquisition. As the market continues to evolve, the rungs on the vendor ladder have changed dramatically. Key players such as BMC, CA, Cisco, HP, IBM, Novell and Oracle have developed, acquired or integrated IdM components to further extend their product offerings. Table 2 demonstrates a selection of the most recent acquisitions:

Table 2. Vendor acquisitions in identity management space

Company	Acquisition
BMC	Calendra and OpenNetwork
CA	Netegrity and Qurb
CA	Infosec's identity and access management solution eTrust
Cisco	IronPort
HP	Baltimore Technologies, Trustgenix, TruLogica and SelectAccess
IBM Tivoli	Access 360
Novell	e-Security
Oracle	Bharosa, Bridgestream, Oblix, Thor, OctetString
Sun	Waveset
Quest Software	Vintela

More recently, identity management is seeing the advent of the "identity suite" vendor. The major players – like IBM, Oracle, HP, Microsoft, Sun and CA – offer an identity "stack" or collection of modular, identity-related products that integrate the functionality of traditional IdM solutions with more complex areas like provisioning, federation and virtual directories.

Vendors expect end-to-end suites to support sophisticated provisioning along with the more traditional functionality. Solutions that are built on Web services will also play an increasingly important role in the next few years. Traditional managed PKI vendors, such as Entrust and RSA, are aggressively moving to secure Web services and better re-orient themselves as identity management providers.

The goal of all those acquisitions has been to give users more out-of-the-box identity management features and integration, and such products have been rapidly hitting the market. For example, BMC recently released its Identity Management Suite, which integrates the former Calendra and OpenNetwork software into BMC's identity management package.

The market grows

In spite of high infrastructure cost, reluctance to adopt a new technology and nonexistence of government support, the market for identity management is growing swiftly. And, according to analyst group RNCOS, an unexpected rise in 2005 in incidents of identity theft stimulated the rapid inclusion of identity management solutions in industries.

The strong need for these solutions is evident: IDC has reported that the total worldwide revenue for identity and access management products reached almost US$3 billion in 2006 and is forecast to reach more than US$4.9 billion by 2011. Analyst group Datamonitor also reported significant growth for IdM products and services: revenues are expected to reach US$6.2 billion by 2007.

Vendors are also jockeying for leading market share positions. In its independent July 2007 report, IDC ranked IBM as the worldwide IdM leader for the first time, surpassing CA, which led in 2005. IBM led all other vendors with a 12.2 percent revenue share in 2006, indicating 10.6 percent growth from 2005.

In fact, Digital ID World never expected identity management to evolve as it has. IdM is now an accepted and desired initiative within most major enterprises.

"IDC has ranked IBM as the worldwide IdM leader for the first time, surpassing CA."

The identity management brands

Currently, there are more than 90 vendors offering solutions in the identity management market. These vendors can be broken down into more specific classifications:

- Anchor or generalist brands
- Specialty brands
- Boutique brands

The anchor or generalist brands

Those IdM vendors with diverse product portfolios are classed as anchor or generalist brands. These brands are not linked with any particular market segment. Featured within this brand class are many of the major technology vendors, including:

- EMC
- HP
- Microsoft
- Novell
- Oracle
- Siemens
- Sun

The vendors have made significant investments, mainly through acquisitions, and now provide IdM suite functionality. These companies, with the exception of Microsoft, typically include consulting services as a major selling component. They also rely heavily on their own application platforms as the foundation of their businesses, and as a result, very often align their IdM suites – as well as their other solutions – toward promoting their particular platforms. In doing so, these vendors can leverage the "one-stop shop" idea of providing customers with all the products and services under one roof. IBM and Novell have been strong in this area, with HP and Oracle in chasing roles as their services continue to mature.

Geography can also play a role. While all of these vendors possess worldwide presences, several factors make their products more successful in particular regions. IBM, Sun and Novell are successful in Europe and Asia, where they often compete against specialty brands like CA and BMC. Siemens has a large IdM customer base in Europe with a strong following within the financial services and automotive industries.

For those vendors that rely on their flagship application platforms – Microsoft, Sun and Oracle – these serve as their value proposition. Customers already using Windows, Java or Linux often look to these vendors for their identity management solutions.

The specialty brands

As the name suggests, specialty identity market brands centre on a specific niche market. Vendors in this class generally offer a single product or small group of products to a highly targeted market segment. Among them are EMC, Entrust, BEA and Red Hat.

For example, authentication is a key component in identity management. Therefore, many vendors defer stronger authentication technology to specialist vendors like EMC or Entrust. And while some anchor or generalist vendors do offer these technologies, none are viewed as market-leading authentication products. Vendors such as Entrust or EMC have leveraged their long time experience in stronger authentication and thus have profited from the rapidly growing IdM market. And because the market is so highly competitive, these companies have also moved into federation and policy-based authorization, both of which are expected to show significant future growth.

The boutique brands

The third class of IdM vendors is the boutique vendor. These suppliers work at the category level, within a very specific niche area.

There are several dozen boutique vendors that provide targeted solutions in the IdM space, including provisioning, federation, identity services, password management and ESSO. Currently, about a dozen vendors have also emerged with functionality for role management, including BHOLD and Courion. To date, Ping Identity is the leading boutique vendor for federation.

Yet, here the waters become somewhat muddied. Several boutique brands have grown into self-sustaining, broadly-featured specialty brands with a core identity management focus. This is a new and unsettled area of the market, so the distinction between boutiques and specialty brands in the market is unavoidably shaky. For example, Evidian operates as an identity brand, yet its parent company, Groupe Bull, is a large European anchor brand. And Courion and M-Tech have emerged as identity brands by diversifying their product portfolios and by maintaining large customer bases.

The platform vendors

While application platforms are generally in the realm of anchor or generalist brands like Microsoft and Sun, two specialty brands also focus on platforms: BEA and Red Hat. Using their Java 2 Enterprise Edition (J2EE) and open source Linux respectively, both vendors provide some identity management features.

And with acquisitions high priorities for many vendors, the same holds true for BEA and Red Hat. In 2003, BEA acquired CrossLogix and in doing so, offered Web-based SSO features as part of its BEA WebLogic Server. However, BEA has been all but inactive beyond this point.

Red Hat is a more recent entrant in identity management. With its acquisition of Netscape's enterprise server technologies, the company was able to introduce directory and certificate server products. But once again, the buck has stopped here. The only redeeming factor thus far has been the company's open sourcing of its directory server as part of its Linux distribution. But it still faces a competitive uphill climb, particularly from Novell with its Linux-based identity services.

Identity management vendors

The objective of this section is to review the leading identity management vendor solutions as well as company activities. Where the information is available, the future plans of the various vendors will be indicated.

Activ identity
Web site: http://www.actividentity.com

Born out of the 2005 merger of two established market vendors, Activcard and Protcom, Actividentity has created a one-stop shop for digital ID management. Activcard's main focus within the marketplace was authentication, remote access management and smartcard management systems. Protocom's focus was that of enterprise SSO. The merger was driven by the market need for strong authentication security and the added value SSO provides. The current product lines are solutions for SSO, secure remote access and enterprise access card management. It also provides packages solutions tailored to the enterprise, financial services, healthcare and government markets.

Through an OEM agreement, Actividentity's flagship product, SecureLogin, is a key component of Novell's identity management solution.

Due to the 2006 U.S. HSPD12 presidential directive that requires all new employees to have a common access card, Actividentity was able to score a number of large contract wins, including ABN Amro and Renault. A major contract win featured providing 10 million smartcards for the U.S. Department of Defense and its three branches of the military services.

Actividentity provides organisations with the ability to issue users with a single strong identity. This identity is then authenticated through one or a combination of strong forms in identity. Security is increased because account management is removed from end user control.

Bloor Research's Nigel Stanley gives Actividentity the thumbs up. Because it is built on open standards, it gives companies a better advantage when it comes to creating a secure business with secure physical access, single sign-on and remote access, and all from a single vendor.

Avatier Corporation
Web site - http://www.avatier.com

Established in 1995, Avatier Corporation provides an extended, trust environment and flexible, policy-based user lifecycle management through its flagship Avatier Identity Management Suite. Rather than perimeter control and detection, the modular suite focuses on identity-centric authentication in order to reduce risk.

From a positive standpoint, Avatier provides good password management, single sign-on, provisioning and de-provisioning and administrative capabilities. It offers extensive helpdesk system support, although it has been noted by analysts, including the Butler Group, that the suite has poor support for third party Web access control systems. The company states that the suite is very suitable for small to medium-sized enterprises (SMEs) containing upward to 200 end users, yet the product has seen successful deployments in 200,000-user environments, making it a highly scalable solution for the larger enterprise market.

Aberdeen Group also interviewed IT managers regarding Avatier's products. These customers reported that Avatier's products pay from themselves in one to two months. The software is installed and operating in less than an hour, with many quoting times of five to ten minutes. IT managers also stated that they have seen reduced technology and procedural complexity and fewer problems with local user account control.

Analyst groups such as Butler Group expect Avatier's European presence to increase significantly through 2007, despite the fact that the company is U.S. based.

BMC Software
http://www.bmc.com

BMC is taking a multifunctional product approach to identity management, now claiming more than 800 customers using its IdM solutions. The company has increased its coverage in the IdM market through its Calendra and OpenNetwork acquisitions. With the technologies from these companies, BMC added Web access management (WAM), directory management and virtual directory services to its feature list. In addition, BMC has formed partnerships with Consul and Passlogix for risk management and ESSO respectively.

The acquisitions were greatly needed because BMC had, as Gartner reported in its Magic Quadrant for User Provisioning report, "lost significant 'mind share' during the past three years or so because of its lack of useful workflow and other identity management components, primarily Web access management." With the Calendra acquisition, BMC was able to provide good workflow as well as a directory-centric application development environment. The OpenNetwork acquisition gave the company WAM and user provisioning products for both the Microsoft and heterogeneous IT infrastructure. As a result, BMC was able to introduce a .NET offering, making it the first suite vendor to have both .NET and Java user provisioning products. The company now is able to provide end-to-end identity management with strong workflow capabilities.

BMC has partnered with Consul Risk Management to deliver broader audit and compliance reporting capabilities. BMC also markets its user provisioning offering with integration to some of its business services management product line for ITSM support.

The company plans to increase its identity management to further build on its Business Service Management solution capabilities.

CA
Web site: http://www.ca.com

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. Its extensive suite of products not only creates an end-to-end solution, but its broad workflow allows enhanced automation of processes. Its SSO capabilities help reduce risks associated with multiple user passwords.

To its credit, 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 identity management customers.

Butler Group predicts that CA will remain one of the leading market vendors. The company plans to provide wider support for Security Assertion Markup Language (SAML) in its identity federation, as well as support for Microsoft's browser federation solution. CA also plans enhancements to its compliance-related functionality.

Cisco Systems
Web site: http://www.cisco.com

Cisco Systems has been positioned as a global leader in the provision of Internet networking solutions. Its trust and identity management technology is comprised of three solution categories: identity management, identity-based networking services and network admission control. Cisco identity management solutions work to guarantee the identity and integrity of every user on a network. Appropriate access policies are applied so customers can gain visibility into their network activities. Their IdM solutions also allow for centralised and secure management of remote devices accessing networks, and provide authentication, authorisation and accounting functionality across all network devices.

Cisco's Identity Based Networking Services increases network security by automatically identifying users requesting network access. It routes them to a VLAN domain with an appropriate degree of access privilege based on policy and prevents unauthorised network access from wireless access points.

The company's Network Admission Control allows network access only to trusted endpoint devices that can verify their compliance to network security policies. Network access to any device can be allowed, denied, or restricted. It can also quarantine non-compliant devices.

Courion Corporation
Web site: http://www.courionsolutions.com/products

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 to include solutions for not only password management, but user provisioning and account management, profile management, automated digital certificates and compliance.

Courion has a respectable share of the IdM market, with more than 300 customers who have deployed some portion of their Enterprise Provisioning Suite to more than six million users. In order 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.

Courion is also the only boutique vendor to be named in Gartner's Magic Quadrant for User Provisioning. This makes a strong statement about their product and market presence. In his "identityman" blog, Identropy founder and Director of Identity Management Ashraf Motiwala writes, "The fact that they (Courion) could play with the bog boys is notable, and I've seen a lot of clients asking more about their products lately."

According to Courion customer Tim Callahan, SunTrustBanks group vice president in charge of access control and support services, nearly a thousand bank employees used to spend part of each day retrieving or resetting users' passwords – the equivalent of 60 full-time positions. Since implementing Courion IdM suite, the company has slashed that number by 75 percent.

The company has been working to develop self-service productivity aids as well as additional capabilities for compliance.

EMC/RSA
Web site: http://www.emc.com

Prior to 2006, EMC was known largely for its backup and storage solutions. The company also offered several virtualisation solutions, including VMware. However, in 2006, EMC acquired Authentica, a digital rights management vendor; RSA, an authentication and IdM vendor; and Network Intelligence, a security event monitoring vendor. The company plans to combine the technologies to deliver "information-centric security", marketing the solutions under the RSA brand.

RSA's products help organisations protect private information and manage the identities of people, devices and applications accessing and exchanging that information.

Entrust
Web site: http://www.entrust.com

Entrust is focuses on delivering authentication and authorisation technologies for Web-based, client-server and Web services applications. The company's product line provides protection of digital identities through the use of customisable, risk-based strong authentication. It then goes further to offer corporate policy enforcement through advanced content scanning. Its Entrust IdentityGuard and GetAccess products support a good range of single- and multi-factor certification and independent validation methodologies.

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, and is continuing to increase the options available for user authentication.

Evidian
Web site: http://www.evidian.com

Previously known as Bull 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 identity management software suite that focuses on both Web and legacy environments. The company recently consolidated its products into AccessMaster, an IdM suite with nine independent, integrated modules for provisioning, certificates, workflow and secure access.

Unlike vendors with comparable identity management products, Evidian builds all its IdM products internally and offers tighter integration among product components. Evidian claims more than 160 IdM product customers, most of whom are located in Europe and Asia. The company is expected to continue its ongoing success in the European IdM market.

Fischer International
Web site: http://www.fischerinternational.com

Fischer International differentiates itself from other user provisioning vendors by enabling identity management to be delivered by service providers, global outsourcers and internal shared services organisations. This is accomplished though a hosted, Software as a Service (SaaS), an on-premise managed identity service, or as a traditional deployment. According to Gartner, Fischer's technology provides substantial benefits and enables new opportunities for both end-user organisations and service providers.

Fischer is a relatively new vendor in the user provisioning market space. Fischer's user provisioning product, Fischer Identity Suite, was designed and developed from "the bottom up" using a SOA and Java-based architecture. Its ability to discover resources on the network and PDA approval processing support has placed Fischer International among the niche players in Gartner's Magic Quadrant for User Provisioning. While its attestation reporting, enterprise-level role management and SPML are lacking, it more than makes up for these with its SOA framework and aggressive pricing, making it an attractive proposition to the SMB market.

HP
Web site: http://www.hp.com

In 2003, HP began a serious venture into identity management with the purchase of the Select Access technology from Baltimore Technologies. HP then went on to acquire Baltimore Technologies outright along with provisioning vendor TruLogica. The company has since introduced audit and compliance solutions for its IdM suite.

As a vendor with a global presence, HP is now competing with the major IdM players. However, with its strong technology acquisitions, the company has struggled to challenge the anchor or generalist brands, a situation that it can easily rectify. The company's ongoing introduction of extensive professional services aligned with its product offerings is expected to help move it forward.

Although HP is also a platform vendor of HP-UX and NonStop, the company's IdM solutions show no sign of favouritism for in-house platforms. That portfolio currently contains the following products:

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

Like Oracle, HP is one of the more recent entrants into the competitive identity management market, choosing carefully and selectively the companies, technologies and alliances it believes would provide a viable and competitive offering that is also complementary and compatible with corporate strategy.

HP bases Select Identity's key differentiator on their Service Model, that is, the ability to abstract users and roles from provisioned resources and provide management groupings for roles, rules, inheritance, multiple roles, cross-organisational/functional roles, forms and workflows. The company is very active in standards efforts and is considered a thought leader in future developments regarding identity management design.

HP has not been as aggressive as Oracle with its identity and access management suite, choosing a more focused marketing approach to larger customers. However, customers would like to see more development capability integrated in Select Identity, as well as an overhaul of the Business Services model of the product for 2008 and rapid development add-ins in the workflow processes for proof-of-concepts and pilots.

Its Select Identity can play a role in ITSM, such as service life cycle management, resource discovery, help desk, and configuration management and database operations.

IBM
Web site: http://www.ibm.com

IBM entered the competitive identity management market in an aggressive manner, 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, and has in fact just overtaken CA for the top place as worldwide IdM leader in market shares.

IBM has significant resources for research and development 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 organisation for functional and business processes support. And although IBM sometimes hesitates on various specifications efforts – in particular, Liberty Alliance – 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.

Imprivata, Inc.
Web site: http://www.imprivata.com

Imprivata is an appliance-based authentication and access management company that solves the complex problems of managing employee identities, strengthening corporate security and achieving regulatory compliance. The company mainly addresses the SME space for identity management solutions, believing that this market has been poorly served by many other vendors.

Its Imprivata OneSign appliance solution secures desktops, networks and applications, and helps organisations increase their security and replace Windows-based passwords with a range of strong authentication methods. It also unifies enterprise security management by integrating network and building access systems.

Positioned in Leaders Quadrant of Magic Quadrant for Enterprise Single Sign-On (ESSO), Imprivata was found to be “an easy choice for many small and midsize businesses, financial institutions, healthcare organisations and governments.” However, a lack of scalability is still the chink in Imprivata's armor. Failover is not provided among multiple appliance pairs, and separate appliance pairs may need to be deployed and managed for thousands of users across multiple geographies or business units. Imprivata plans to address this issue in 2007, but it currently remains a concern for large clients considering such alternatives. *Journal of Identity Management* editor Dave Kearns reports that the company has added new adaptors to help address these issues.

Microsoft
Web site: http://www.microsoft.com

Microsoft was one of the first anchor or generalist brands to invest in identity management, leveraging both acquisition and development activities. Its Active Directory (AD) is now in use in nearly every enterprise. However, Microsoft's IdM solutions based on AD have been slow in coming and so far have not competed well with other IdM components like WAM and password management.

Its meta-directory and provisioning solution, Microsoft Identity Integration Server (MIIS), has fared relatively well. Now rebranded as Identity Lifecycle Manager (ILM), this is Microsoft’s platform for identity synchronisation, certificate and password management, and user provisioning The company’s work on federation and certificate services will likely attract widespread use.

Microsoft had cultivated a small community of boutique vendor partners that actually extended the reach of MIIS and AD beyond the traditional Microsoft borders. Though a reasonable approach, it has not proven to be sustainable. Vendors such as OpenNetwork, Vintela and Oblix were acquired by vendors, or rather, competitors, less committed to Microsoft's collaborative strategy.

M-Tech IT
Web site: http://mtechit.com/

Headquartered in Calgary, Alberta, Canada, M-Tech IT's approach is to streamline user provisioning and password management processes. In doing so, the company provides organisations with improved security, regulatory compliance and a rapid return on investment.

While its flagship product is its P-Synch for password management, the company also released an identity management suite for mid- to large-sized enterprises. The M-Tech Identity Management Suite is strong in user access, regulatory compliance and certificate management, account discovery and interactive voice response authentication.

Novell
Web site: http://www.novell.com

Novell has been developing and building out its IdM suite since the mid-1990s. The company currently offers integrated products for directory services, access management, provisioning, meta-directory services, password synchronisation, Web and enterprise single sign-on, user management 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, the first product to provide support for federation, Web resource access, enterprise application access, single sign-on, applications and directory structures.

In his blog, Neil Macehiter, Research Director of Macehiter Ward-Dutton reported his company's first IdM infrastructure assessments using Novell. Macehiter writes, "Novell's offerings are a sensible choice for organisations with an existing investment in eDirectory or who are focusing on identity lifecycle management or user-mediated single sign-on."

Oracle
Web site: http://www.oracle.com

Already a globally recognised brand in database, middleware and business applications, Oracle has used a series of acquisitions to further strengthen its business application position and to place a new emphasis on the identity management market with its Fusion Middleware strategy. Oracle is now be viewed as a major IdM suite provider, based on its size, global reach, along with the acquisitions of Oblix, Phaos Technology, OctetString and Thor Technologies. These acquisitions brought additional capabilities to its portfolio.

Oracle's future success depends on how well it executes a strategy that is fundamentally different from its previous delvings into IdM. Previously, Oracle provided IdM capability that was tightly bound to its Oracle Internet Directory (OID) product and offered little flexibility in deployment options. With its new strategy built around a Fusion Middleware stack of components, Oracle is embracing industry standards and is planning to support additional third-party identity products.

Due to its leading presence in business application and database systems, Oracle is in a position to further advance the industry's progression of adding identity capabilities to applications and platforms. Many competitors still provide IdM as an add-on to application server functionality or to a business application. This view of IdM gives Oracle an opportunity to upsell identity products, while offering enterprise business applications. Oracle needs to remain focused and be consistent in its product messaging to avoid confusing customers.

Oracle's biggest challenge will be to present a value proposition that sets it apart from leading identity management vendors like BMC, CA, IBM and Sun. Recent breaking news suggests that Oracle has made a significant cash share bid to acquire BEA. Should this occur, a combined Oracle and BEA will offer a strategic blow to all three of Oracle's main competitors: IBM, SAP and Microsoft and drive a possible and deeper IBM/SAP alliance. All major IdM vendors will be carefully watching events as they progress.

Ping Identity
Web site: http://www.pingidentity.com

A leading boutique vendor for federation, Ping Identity specializes in Web-based SSO products and identity management for Web services. An interesting company approach comes in the fact that Ping Identity allows prospective customers to download its products at no cost, and then use them for 100,000 transactions or 12 months before payment in due.

Its two flagship products are PingFederate, a stand-alone federated identity server, and PingTrust, a solution that provides integration of federated identity with Web services.

The company more recently launched PingLogin, a middleware product that's written in Java. PingLogin allows various methods of strong identity authentication, such as the use of smartcards and biometrics, for access to applications.

Quest Software, Inc.
Web site: http://www.quest.com

For a number of years, Quest Software has offered identity management tools for Microsoft's Active Directory management and migration. Quest's recent acquisition of Vintela, a company that provided Active Directory features to the UNIX and Linux environments, makes Quest a vendor both for runtime and background identity management.

SAP
Web site: http://www.sap.com

SAP is a major provider of business software, including solutions for enterprise resource planning (ERP), supply chain management and customer relationship management. SAP's 2006 acquisition of Virsa Systems brought to the company an enterprise application controls management vendor offering access control and separation of duties features for the ERP environment. Rebranded as SAP Governance, Risk, and Compliance (GRC) Access Controls, the solution is integrated with SAP's new governance, risk and compliance (GRC) Web services. Based on open standards and built on SAP's NetWeaver platform, the new Web services extend the full capabilities of SAP GRC Access Control, allowing identity management software vendors to tightly integrate their respective solutions, and providing customers with a single set of tools to efficiently and cost-effectively manage user identities, enforce corporate security policies and ensure compliance with regulatory mandates. The enhancements come through SAP's acquisition of MaXware, a privately held provider of identity management software.

Most obviously, SAP's acquisitions bring additional consolidation and competition to the IdM market, particularly with its NetWeaver, SOA, standards and identity strategies. There is strong potential to influence the idea of identity as a service, one that SAP can have the opportunity to leverage. However, to be successful, SAP must take the time to understand the needs of its current and prospective customers.

Siemens
Web site: http://www.siemens.com

Siemens is a longtime player in the identity management market, having released its directory server product back in 1991. The company went on to deliver meta-directory services and provisioning products. Siemens currently enjoys a significant market presence in Europe, where the IdM solutions were originally marketed. The company has a strong partnership with SAP and 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.

Sun Microsystems
Web site: http://www.sun.com

Along with vendors Oracle and IBM Tivoli, Sun is one of the major vendors to dominate the user provisioning market. With its acquisition of Waveset Technologies, Sun was able to develop a user provisioning solution that was later chosen as a leader in Gartner's 2006 Magic Quadrant. In addition, the company was able to transform a poorly performing directory-centric business into an extensive identity management suite. It has also added an audit and compliance product to round out its IdM offering.

Identity management is a primary driver for Sun's success in the enterprise software market, and the company has aligned its business plans in support of the now separate IdM business unit. The company's strategy is to provide an identity management solution for high-scale extranets. Its acquisition of identity deployment automation vendor Neogent has further refined its portfolio of rapid implementation capabilities.

However, its user provisioning solutions for mainframe-centric and Windows-centric customers aren't as compelling as some of its competitors' solutions. This can ultimately become more problematic as the identity management market matures and customers needs warrant these solutions.

Sun also recently announced plans to open source its Java Enterprise Systems software, which includes much of the company's identity management suite. This has the potential to be a huge gamble for Sun, because it's unclear whether or not the move will generate additional sales in services or hardware.

Summary

The identity management market is continues to present itself as a rapidly growing space focused on some of today's most critical technology issues: security, compliance, authentication and authorisation. Vendors provide a range of IdM strategies and products, but given the nature of the market, many will find it difficult to dominate the space, and so many areas of identity management may remain fiercely contested. However, enterprises large and small must forge ahead with their identity management initiatives to enable better security, comply with increasing regulations, and audit exactly who is accessing their systems.

Resources

Braunberg, Andrew. *CSO Magazine*, “Market Assessment: Identity Management”, April 2004. http://www.csoonline.com/analyst/report2365.html

Braunberg, Andrew. *CSO Magazine,* “Sun to Open Source Its Identity Management Suite”, December 2005.
http://www.csoonline.com/analyst/report3982.html

Butler Group, *Identity and Access Management: Laying the Foundations for a Trusted Business Environment*, July 2006.

Department of Trade and Industry (UK), *Information security breaches survey 2006,* 2006.

Department of Trade and Industry (UK), *Information security breaches survey 2006: Identity and access management*, 2006.

Fontana, John. Network World, “Compliance pushing identity management in new directions”, September 2007.
http://computerworld.com.my/ShowPage.aspx?pagetype=2&articleid=6453&pubid=4&issueid=121

Frost and Sullivan. *Security Meets Simplicity to Create Trust,* 2006.

Gardner, Dana. ZDNet Blogs, “Oracle roils enterprise vendor landscape with its move to acquire BEA”, October 2007.
http://blogs.zdnet.com/Gardner/?p=2556&tag=nl.e622

Gartner, *Magic Quadrant for Enterprise Single Sign-On*, 2007.

Gartner, *Magic Quadrant for User Provisioning*, April 2006.

IDC, *Worldwide Identity and Access Management 2007-2011 Forecast and 2006 Vendor Shares*, July 2007.

Kearns, Dave. *Journal of Identity Management*, October 2007.

Kearns, Dave. Network World, “Identity discussions at Digital Identity World, Part I”, October 2007.
http://www.networkworld.com/newsletters/dir/2007/1008id1.html

Kearns, Dave. Network World, “Identity discussions at Digital Identity World, Part II”, October 2007.
http://www.networkworld.com/newsletters/dir/2007/1008id2.html

Kearns, Dave. Network World, “Vendors release wares at Catalyst conference”, June 2007.

http://www.networkworld.com/newsletters/dir/2007/0625id2.html

Kilpatrick, Ian. IT-Analysis, “Identity Management: The Growing Challenge”, June 2006.
http://www.it-analysis.com/business/news_release.php?rel=548

Neuenschwander, Mike. Burton Group, *Enterprise Management Market 2006-2007: Not a Winner-Take-All Market*, November 2006.

Penn, Jonathan. Forrester, “Oracle Doubles Down on Identity Management”, November 2005.

Rowland Lori. Burton Group, “SAP acquires MaXware”, May 2007.
http://identityblog.burtongroup.com/bgidps/2007/05/index.html

Smith, Gary E. *SOA Identity Architect,* “SAP Enables Secure, End-to-End Compliant Identity Management”, October 2007.
http://soaidentityarchitect.com/2007/10/03/sap-enables-secure-endtoend-compliant-identity-management.aspx