February 6, 2008

# Identity Management Market Forecast: 2007 To 2014

by Andras Cser and Jonathan Penn
for Security & Risk Professionals

*Includes a market sizing forecast*

February 6, 2008

# Identity Management Market Forecast: 2007 To 2014

## Provisioning Will Extend Its Dominance Of Market Revenues

**by Andras Cser and Jonathan Penn**
with Paul Stamp, Allison Herald, and Alissa Dill

## EXECUTIVE SUMMARY

The identity management — or identity and access management (IAM) — market will grow from nearly $2.6 billion in 2006 to more than $12.3 billion in 2014 (including revenues from both products and implementation services). Provisioning accounts for half of IAM market revenues today, but it will account for nearly two-thirds of all IAM revenues by 2014. Even after years of healthy adoption rates, the IAM market is actually just beginning its trajectory toward broad adoption and deep penetration. Moreover, during the next seven years, we will also see buying behavior migrating from point products to identity suites — and, to a lesser extent, from products to managed services. Meanwhile, vendors will decompose products into service-oriented architecture (SOA)-enabled functions, repackaged in the form of identity-as-a-service (IDaaS).

## TABLE OF CONTENTS



## NOTES & RESOURCES

Forrester interviewed 13 vendor and user companies, including: BMC Software, CA, Citrix Systems, Cyber-Ark Software, Hewlett-Packard, IBM, Mycroft/Talisen, Novell, Oracle, Passlogix, Sun Microsystems, and Symark Software.

### Related Research Documents

"User Account Provisioning For The Midmarket"
August 20, 2007

"Trends 2007: Physical And Logical Security Convergence"
August 17, 2007

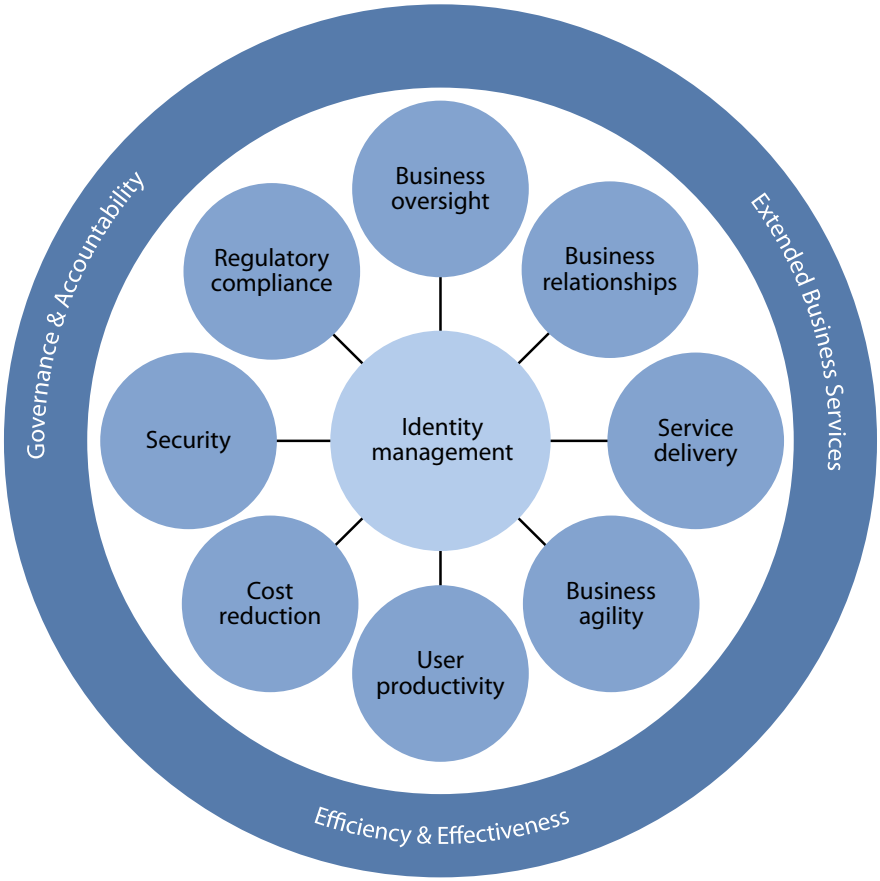
"Identity Management Architecture"
September 18, 2002

## IDENTITY MANAGEMENT LIES AT THE CORE OF PROACTIVE SECURITY

Identity management is not a single product but a set of processes and supporting technologies for maintaining a person's complete set of identity information, spanning multiple business and application contexts. Identity management unifies a person's disparate identity data to improve data consistency, data accuracy, and data and systems security in an efficient manner.[1]

Robust identity management requires both integration of technologies as well as coordination with the IT and business processes surrounding the management of user information, access rights, and related policies. Identity management has successfully thrived amid IT and business change precisely because of its composite nature and multiple benefits. IAM helps extend business services, improve efficiency and effectiveness, and allow for better governance and accountability (see Figure 1).

**Figure 1** Business Drivers For Identity Management



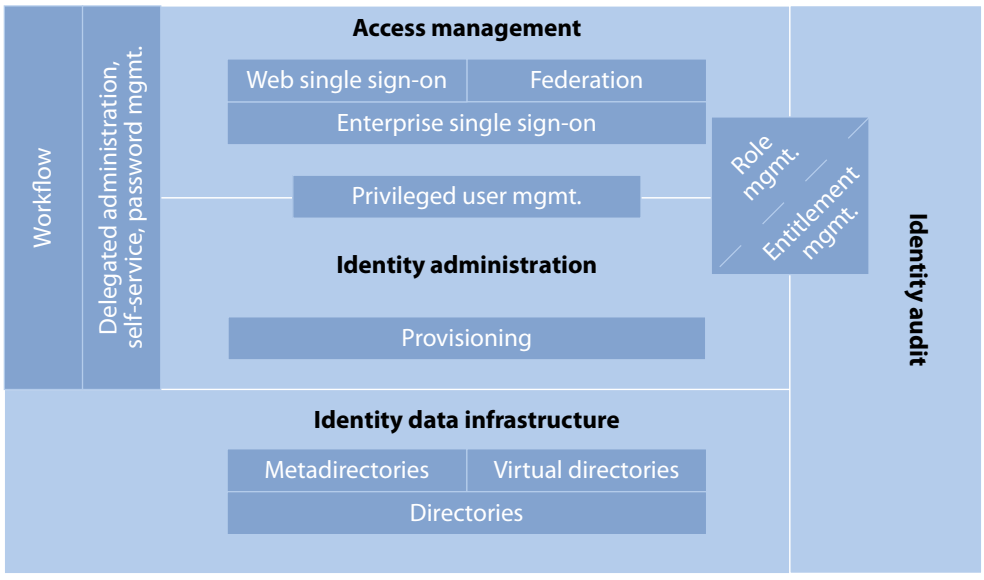

43842 Source: Forrester Research, Inc.

## Identity Management Is A Market Of Distinct But Coordinating Products

The IAM ecosystem combines several types of technologies that (see Figure 2):

- **Establish an identity data infrastructure.** This segment encompasses products that form the identity information layer itself: directories, metadirectories, and virtual directories.
- **Administer accounts and privileges.** Products that manage users' accounts, attributes, and credentials include provisioning, role management, password management, and privileged user management. This category also includes the functional elements of self-service and delegated administration.
- **Control access to IT resources.** Coordinating users' access to multiple applications is the domain of products like enterprise single sign-on (E-SSO), Web single sign-on (Web SSO), and federation. It also includes the emerging area of entitlement management.
- **Audit the administrative and access activities.** Organizations require the ability to demonstrate that account administration and access controls are performing according to policy; identity audit products help with this effort. This includes auditing tools that combine and correlate activities and events across the identity infrastructure, as well as privilege attestation — tools to aid the act of certifying that the privileges associated with a user are correct. It also includes role management products, which serve a dual role of both codifying policies and validating their enforcement.

**Figure 2** The Identity Management Ecosystem




43842 Source: Forrester Research, Inc.

Forrester has not included strong authentication in and of itself (e.g., smart cards, tokens, digital certificates, and biometrics) or variants (risk-based authentication) in this IAM market forecast. These credentials and systems are valuable contributors to identity management and part of the identity ecosystem, but this identity management forecast focuses specifically on the technologies outlined above, not on the overall ecosystem.

## Large Vendors Have Portfolios Of Established Products, While Small Vendors Innovate

In the past, IAM tools were notorious for leaving significant integration headaches for the customer or systems integrator. However, during the past three years, organizations have gradually shifted their interest toward an integrated IAM suite (see Figure 3). Within these suites, functional coordination among products is ironed out during quality assurance (QA) by the vendor — and, preferably, prior to the purchase of the product. Large enterprises are looking for well-oiled, interoperable, and feature-rich protocol stacks and are keen to negotiate license deals that allow for: 1) use of all products in the suite, and 2) an unlimited number of users and servers.

**Figure 3** The Identity Management Vendor Landscape

**3-1 Major identity management suite vendors**

| Vendor | Directory | Metadirectory | Virtual directory | Provisioning | E-SSO | Web SSO | Federation | Privileged user mgmt. |
|---|---|---|---|---|---|---|---|---|
| BMC Software | ○ | ○ | ○ | ● | ● | ● | ● | ○ |
| CA | ● | ○ | ◑ | ● | ● | ● | ● | ◑ |
| Evidian | ○ | ○ | ○ | ● | ● | ● | ◑ | ○ |
| Hewlett-Packard | ○ | ○ | ○ | ● | ○ | ● | ● | ○ |
| IBM | ● | ● | ○ | ● | ● | ● | ● | ◑ |
| Microsoft | ● | ● | ○ | ● | ○ | ○ | ● | ○ |
| Novell | ● | ● | ◑ | ● | ● | ● | ● | ○ |
| Oracle | ● | ◑ | ● | ● | ● | ● | ● | ○ |
| SAP | ○ | ● | ● | ● | ○ | ○ | ○ | ○ |
| Siemens | ● | ● | ○ | ● | ○ | ○ | ○ | ○ |
| Sun Microsystems | ● | ● | ● | ● | ○ | ● | ● | ○ |

● Yes ◑ Some ○ No

43842 Source: Forrester Research, Inc.

**Figure 3** The Identity Management Vendor Landscape (Cont.)

**3-2 Identity management specialties**

| Specialties | Vendors |
|---|---|
| Provisioning | • Avatier<br>• Beta Systems Software<br>• Courion<br>• Fischer<br>• M-Tech Information Technology |
| Web SSO and federation | • Entrust<br>• Ping Identity (federation only)<br>• RSA Security<br>• Symlabs (federation only) |
| Enterprise SSO | • ActivIdentity<br>• Citrix Systems<br>• Encentuate<br>• Imprivata<br>• Passlogix<br>• Sentillion |
| Privileged user and password management | • Cloakware<br>• Cyber-Ark Software<br>• eDMZ Security<br>• Symark Software |
| Virtual directory | • Radiant Logic<br>• Symlabs |
| Role management | • BHOLD<br>• Eurekify<br>• Proginet<br>• Vaau (acquired by Sun Microsystems) |
| Entitlement management | • Securent<br>• Vanguard Integrity Professionals |
| Identity audit | • Aveksa<br>• NetVision<br>• SailPoint Technologies |

43842 Source: Forrester Research, Inc.

## THE IDENTITY MANAGEMENT MARKET WILL EXCEED $12 BILLION BY 2014

The overall size of the worldwide IAM market — based on software license (including maintenance) and related implementation service revenues — reached approximately $2.6 billion in 2006, with 48% of revenues going to software and 52% going to the services that IAM product vendors and system integrators (SIs) delivered. By 2014, total revenues will reach $12.3 billion, with 57% going to software and 43% going to services. The compound annual growth rate (CAGR) of the entire IAM market during the 2006 to 2014 period will be 21.6% (see Figure 4).

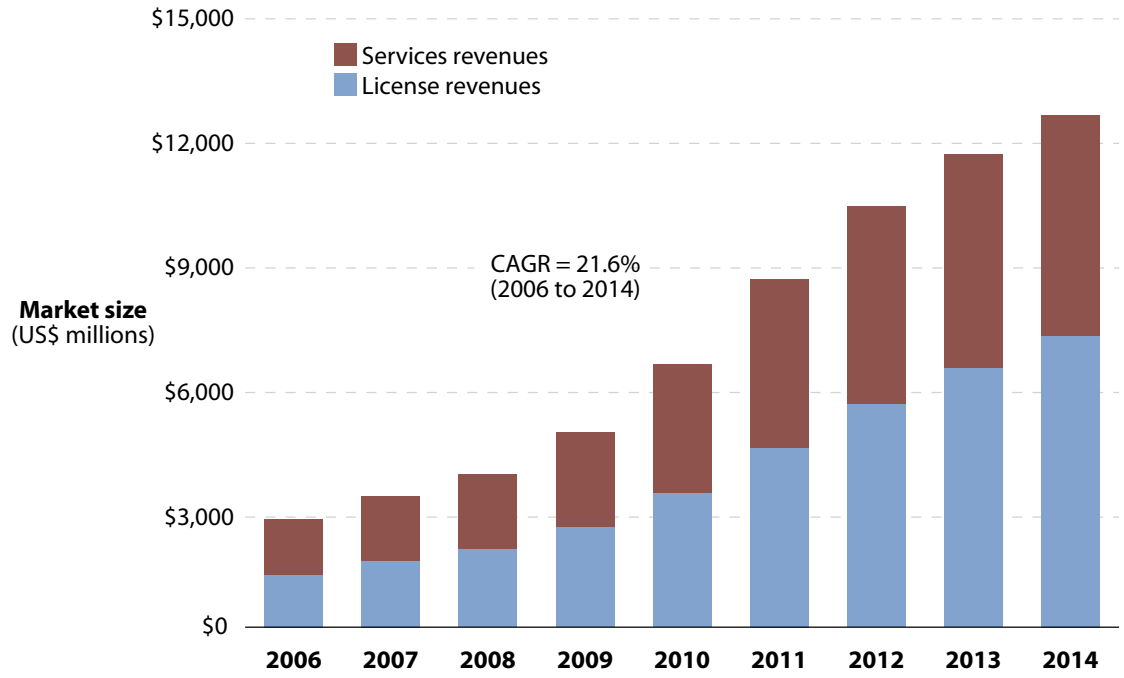
Provisioning — with license and related implementation services combined — accounted for 50% of all IAM revenues in 2006 and is growing at a CAGR of 25.4% (see Figure 5). Other product segments that are major contributors today to IAM market size are Web SSO, E-SSO, and directories (see Figure 6). By 2014, provisioning will account for 64% of all IAM market revenues, dwarfing all other components as it further penetrates the enterprise landscape, makes inroads into the midmarket, and continues to require significant consulting and integration investment for implementation. E-SSO adoption will also rise significantly over this period, from roughly $250 million to $2 billion — a CAGR of 28.5%. The other major element of IAM revenues will be Web SSO — increasing only modestly from today at a CAGR of 6.9% but still contributing more than 9% of the total market size.

Enterprises in North America lead the global adoption of IAM; they account for 67% of the market today, with Europe accounting for 26%, and Asia Pacific for 6%. IAM adoption in North America will continue to fuel overall revenue growth, but above-market growth will occur elsewhere within the next seven years. By 2014, North America will account for 60% of the IAM market, Europe 27%, and Asia Pacific 8% (see Figure 7).

**Figure 4** Forecast: Global Identity Management Growth, 2007 To 2014, License Versus Service

**Total IAM application market by license (including maintenance) versus services revenues**

The spreadsheet detailing this forecast is available online.

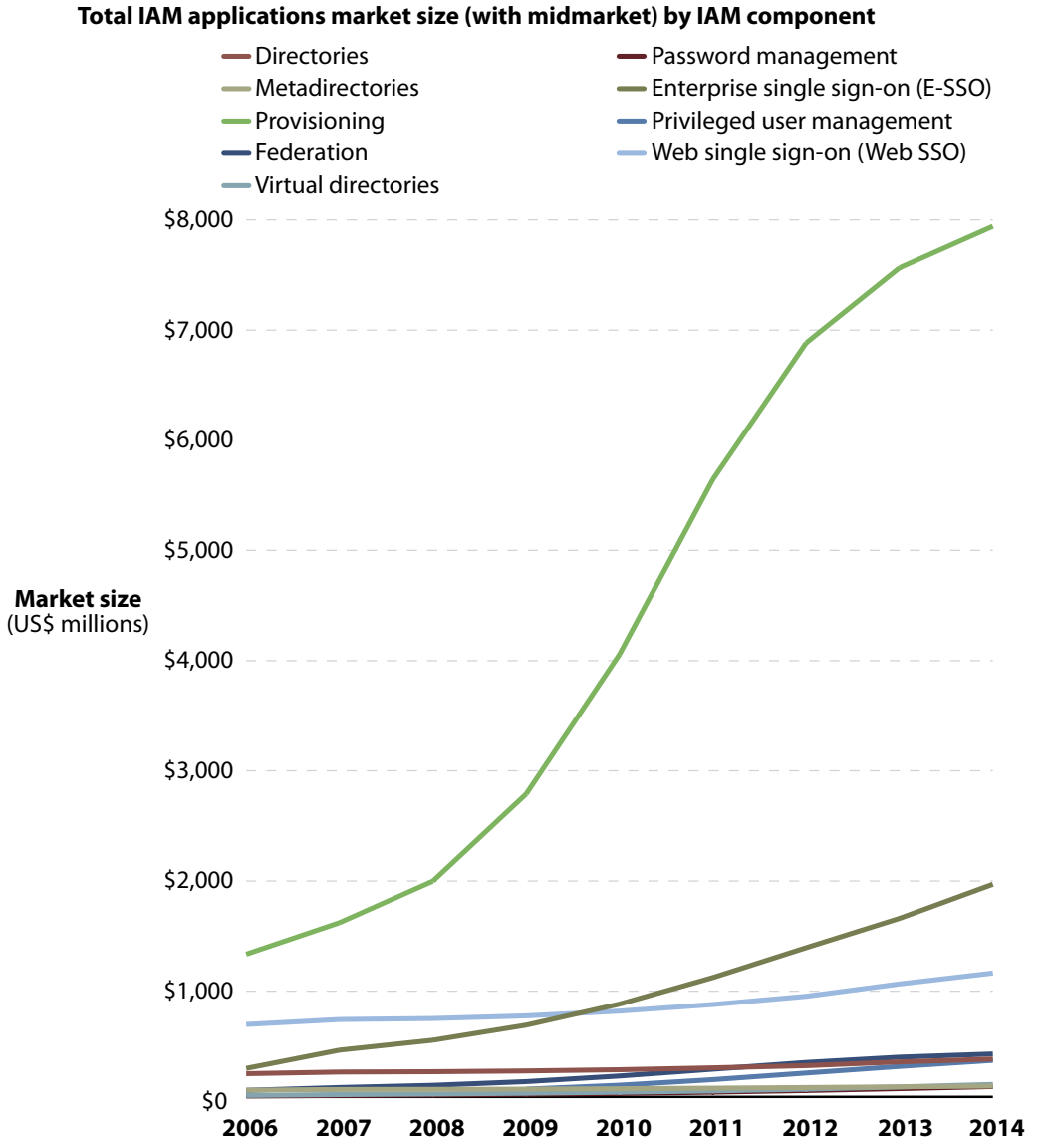



43842

Source: Forrester Research, Inc.

**Figure 5** Forecast: Global Identity Management Growth, 2007 To 2014, By Component

The spreadsheet detailing this forecast is available online.

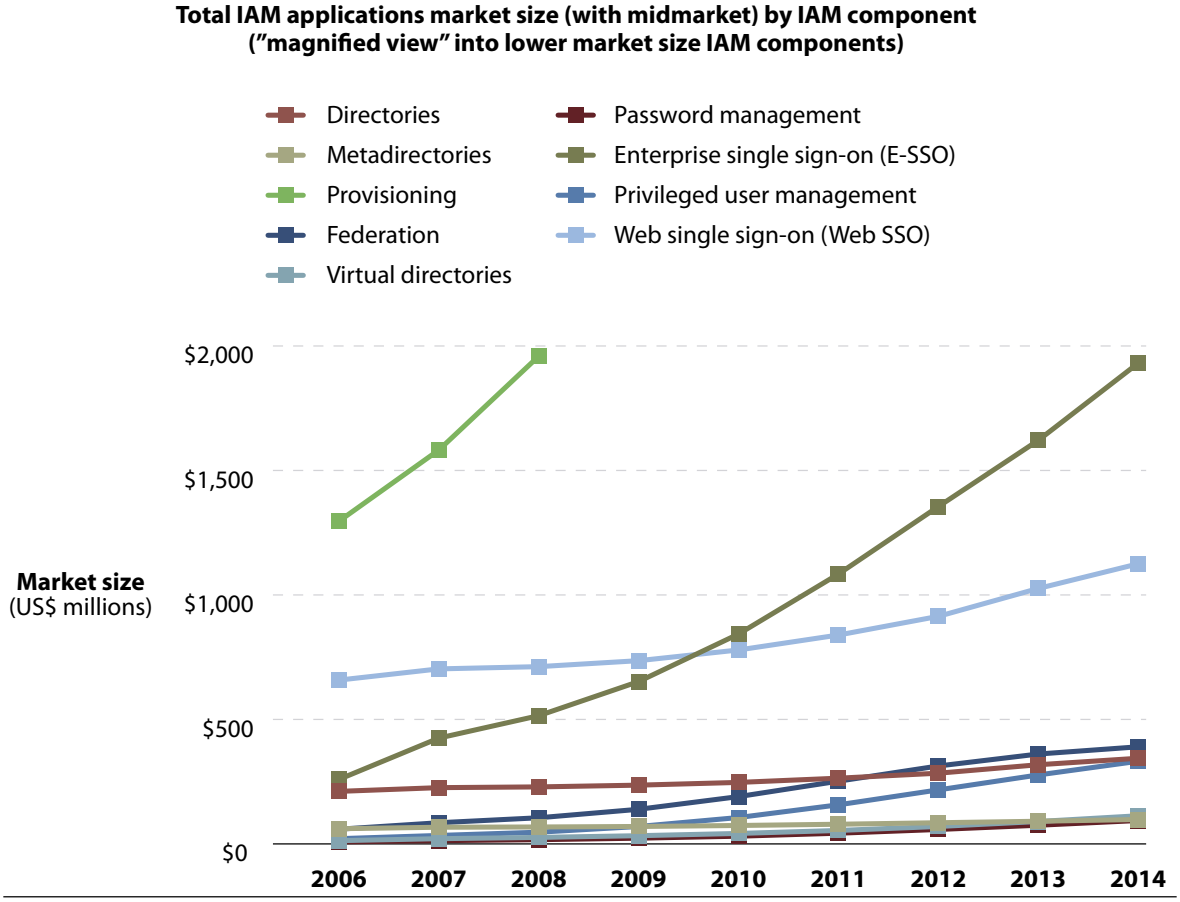



| | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|---|---|---|---|
| Provisioning | $1,296 | $1,582 | $1,959 | $2,750 | $4,017 | $5,605 | $6,844 | $7,526 | $7,902 |
| Web SSO | $658 | $703 | $712 | $736 | $779 | $839 | $914 | $1,026 | $1,125 |
| E-SSO | $259 | $425 | $515 | $652 | $843 | $1,084 | $1,355 | $1,621 | $1,931 |
| Directories | $211 | $226 | $229 | $236 | $247 | $264 | $284 | $318 | $344 |
| Metadirectories | $61 | $67 | $68 | $70 | $74 | $79 | $85 | $91 | $98 |
| Federation | $59 | $85 | $105 | $139 | $190 | $252 | $313 | $361 | $390 |
| Privileged user management | $21 | $34 | $47 | $70 | $106 | $157 | $217 | $277 | $332 |
| Virtual directories | $13 | $21 | $26 | $33 | $42 | $54 | $70 | $90 | $113 |
| Password management | $8 | $13 | $17 | $23 | $31 | $43 | $58 | $75 | $94 |

43842 Source: Forrester Research, Inc.

**Figure 6** Forecast: Global Identity Management Growth, 2007 To 2014, By Component (Magnified)

The spreadsheet detailing this forecast is available online.

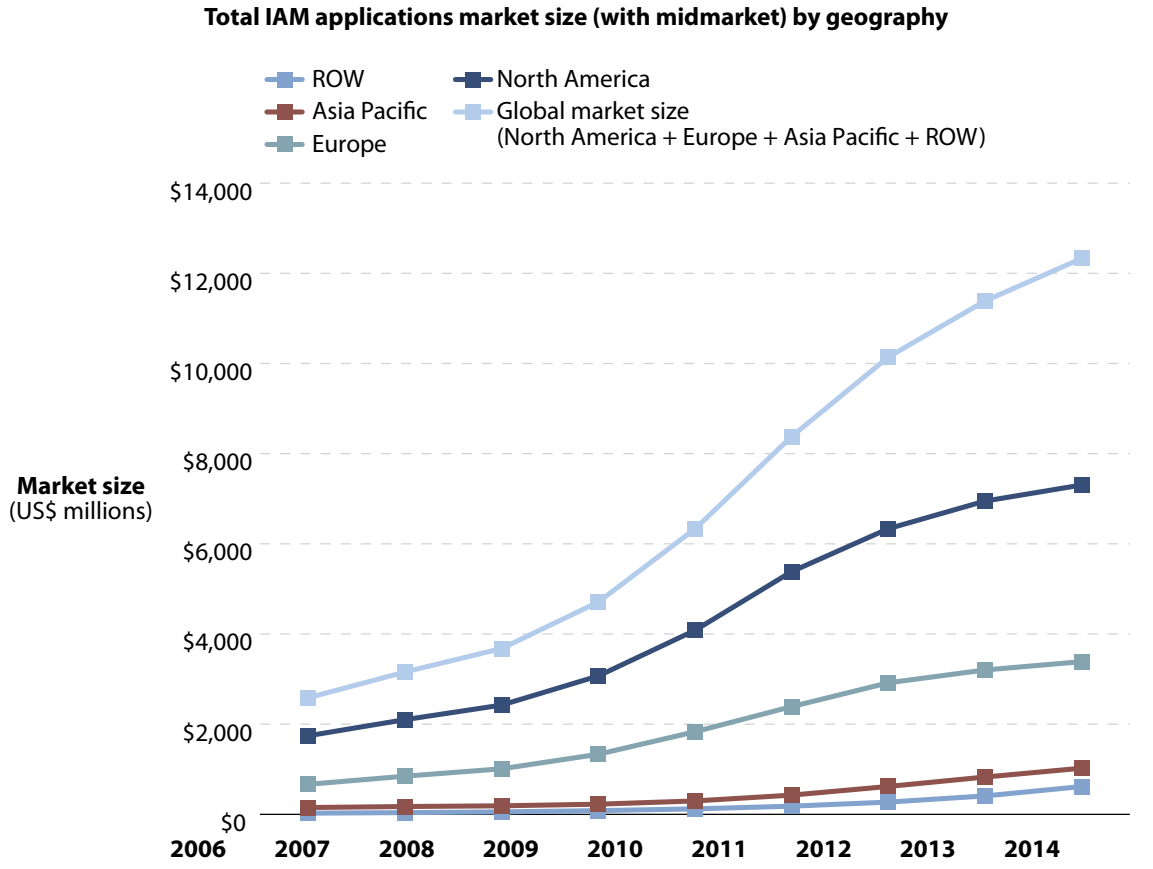



43842 Source: Forrester Research, Inc.

**Figure 7** Forecast: Global Identity Management Growth, 2007 To 2014, By Geography

The spreadsheet detailing this forecast is available online.




43842 Source: Forrester Research, Inc.

## FUTURE DIRECTIONS FOR IDENTITY MANAGEMENT

Today, compliance is the major driver behind adoption — organizations need to build a control framework for managing who has access to what, why they have that access, and what they're doing. A substantive and emerging driver, though, is the protection of corporate information assets. As new trends emerge, the definition of the identity management market is sure to change and the market will expand. We can already see several forces that are likely to influence the market in significant ways during the next few years, including IT governance, compliance, integration with business process management, and the rise of IAM suites over point products as the dominant approach to implementation. IAM vendors also identified the following trends as shaping the market in the next five to seven years:

- **Identity-as-a-service (IDaaS).** IDaaS is a concept similar to software-as-a-service (SaaS). Instead of relying on the monolithic, largely product-centric implementation of identity management, IDaaS decomposes the functions within IAM products and offers a modular and

coherent set of services for managing access, identities, provisioning, policies, and entitlements. The greatest benefits of IDaaS — as with SaaS — are code reuse, easier integration of IAM into IT infrastructure and applications, and lower total cost of ownership. A few vendors — most notably CA, Oracle, and Sun Microsystems — have been articulating such a strategy, although none are far along in execution.

- **Outsourced identity management.** When regulatory requirements force them to adopt identity management, small and medium-size businesses — and even smaller enterprises — may not possess all of the resources to implement all aspects of it in-house.[2] This explains the rise of outsourced identity management, which Forrester expects to reach maturity in 2009 to 2010. Compuware/Covisint, Mycroft/Talisen, Oracle/Wipro, and SAFE-BioPharma offer the outsourcing of identity management and, in some cases, the establishment of networks of trust. We expect to see more industry-specific offerings in this space, allowing server message blocks to convert capital IAM expenses into recurring operating expenses.

- **Centralized, fine-grained entitlement management.** A number of factors dictate whether a user can have access to a specific application functionality or resource. These factors include user attributes, group memberships, application context (e.g., the amount of money the user is trying to transfer in a financial application), and how the user is trying to access the resource (e.g., is the user accessing the application from North Korea at 3 a.m. Eastern Time or from New York City at 10 a.m.?). For large enterprises, managing collaboration, portal applications, and databases in a manner that enforces segregation of duty not only within one area but also between lines of business is also of major concern. BEA Systems, CA, Securent, and Vanguard Integrity Professionals are the key players in this market, with Securent (which Cisco recently acquired) being the emerging leader. As entitlement management can be implemented successfully without identity management, we expect it to pull larger IAM implementations in the future.

- **Consumer identity solutions for proofing and authentication.** Verifying the identity of people enrolling in online services is a challenge. The identity verification process today is largely based on financial information. However, this makes an individual's financial data not only a target of theft in itself but also a factor in subsequent identity theft. Related to this, many organizations with loose relationships with their customers or users can benefit from using what is known as user-centric identity. With user-centric identity, the consumer selects a third party that vouches for his or her identity to the organization. Examples of user-centric identity include OpenID and Microsoft's CardSpace. With credit card and identity theft on the rise, Forrester expects identity verification solutions to become mainstream for healthcare and financial services online enrollment processes. The future of user-centric identity is less certain, but it could exert a significant influence if a large portion of the population has easy access to digital credentials that popular commercial Web sites deem trustworthy.

- **Policy repository convergence.** After organizations define their global governance, risk, and compliance (GRC) policies and controls, they spend surprisingly vast amounts of resources translating these policies into siloed, product-specific policies, each stored in its own policy repository. Each policy repository contains fairly static information and supports only a segment of IAM: It's clearly a massive challenge for IT to maintain this, especially during a reorganization. Enterprises are striving to unify these policy repositories, and IAM suite vendors have a great opportunity here to meet such needs.

- **Physical/logical security convergence.** Some firms have selectively integrated enterprise physical security controls and management regimes, but Forrester expects such convergence strategies to gradually become mainstream.[3] Many of the areas of attention in such projects focus on identity management: access controls and directories, provisioning, and credentials. A market in which convergence is common would lead to greater strong authentication, single sign-on, and federation.

## RECOMMENDATIONS

### VENDORS AND THEIR INTEGRATORS NEED TO HELP CUSTOMERS WITH IAM STRATEGIES

As customers build out and maintain their IAM strategy and road map, vendors should be involved with: 1) providing a product and suite road map for customers, and 2) answering feature questions honestly. Many IAM implementation fiascos have happened because vendors failed to inform the customer upfront about a certain feature or lack thereof. Vendors need to understand that the context of an organization's IAM strategy and road map is critical for selecting IAM products for the following reasons:

- **IAM should be integrated into a broader security strategy.** IAM will remain an integral part of logical security. While IAM has previously been deployed for specific functions like access rights compliance and portal security, it is gaining recognition as general purpose infrastructure. With this, the IAM buildout is relevant to other aspects of security, such as physical security, information leak prevention, network security, and security information management.

- **The market trend toward suites will complicate product selection.** As IAM continues to comprise new technologies, product suites will embrace these. As the feature jungle expands, IT security organizations will face greater difficulty in mapping requirements to a shortlist of products and finally selecting a product. Complicating this is the fact that more constituents will be involved in requirements gathering and selection — for example, audit departments, legal departments, and business data owners.

- **Technology complexity demands careful process planning and refinement.** Even with the most careful documentation, assessment, and simplification of business processes, organizations will find mapping requirements to IAM product features a laborious exercise. Organizations will seek the vendor whose stack comes closest to meeting their IAM road

map, so expectations are key. To compete effectively, vendors will require an understanding of an organization's dependencies and must provide flexibility as IAM drivers and uses expand and evolve. Vendors must also provide easily accessible frequently asked questions (FAQs), reference architecture blueprints, and implementation and troubleshooting guides to customers to facilitate the early discovery of technology gaps.

- **Expectations will grow as market adoption increases.** Mainstream IAM adoption will cause users to set the bar higher for product ease-of-use and stability — especially in second- and third-generation environments. Solutions that require extensive customization (and not just configuration) will only be acceptable in niche markets, not for mainstream IAM deployments. In addition to a solid architectural design for high performance, common selection criteria will include internationalization and rich, easily customized interfaces that aid users beyond the security team and often beyond IT.

## DESIGN AND SUPPORT IAM WITH MISSION-CRITICAL REQUIREMENTS IN MIND

Organizations sometimes ignore the fact that identity management and access management applications are mission-critical — they are not just a typical business application but part of the interconnected infrastructure.

- **Develop integration both vertically and horizontally.** Buying behavior trends show that the benefits of adopting a single vendor's IAM solution or suite far outweigh the potential downside of not being able get all the required functionality out of a single vendor's product stack. In three years, vendors will be at a competitive disadvantage if they don't have a solution that unifies user management, workflow, roles, identity and policy stores, and audit.

  These efforts must not limit integration to among the IAM components alone. Customers will also scrutinize the IAM suite's integration with the broader IT infrastructure, such as help desk and change and configuration management.

- **Prioritize the development of strong audit capabilities and SIM integration.** Given that regulatory compliance is almost invariably one of the drivers of any IAM project, the suite's integration with audit information, reporting, and security information management (SIM) systems is crucial. After all, producing the reports for auditors, drilling into them in an audit, and finding information to answer their questions is what executive management usually expects from the IAM solution in the first place.

- **Recognize that world-class customer support will always matter.** If a critical bug arises in an external-facing access management system, it can have two — not mutually exclusive — consequences: Not only can it cripple the operation of the site, but it can also cripple its security. Both of these deficiencies can propel the company to headline news. A cornerstone of avoiding situations like this is reliable vendor support through the Web, phone, email, and chat, employing knowledgeable, engineer-level resources.

- **Get creative with pricing and packaging.** Organizations will ask for more flexible pricing schemes, such as site licenses, subscription licenses, fixed fees for initial deployments combining products and services within the defined boundaries of a project's scope, and unlimited use to manage partners and their customers.

WHAT IT MEANS

## SIMPLIFYING BOTH ACCESS AND ACCESS RIGHTS MANAGEMENT FUELS MARKET GROWTH

Provisioning and E-SSO will interact and pull each other into new accounts. Young provisioning projects will appreciate the immediate ease-of use benefits that E-SSO brings to them and end users, while IT folks will rejoice at not having to modify legacy business applications for E-SSO integration. Once this system helps address auditors' concerns, questions around identity life-cycle management will almost invariably arise — leading to planning for job roles and quickly bringing identity audit, provisioning, and Web SSO into the mix.

### Entitlement Management Growth Will Consume Some Of Provisioning's Dominance

Provisioning embodies the fundamental task of security administration and, as such, will remain a critical element of the IAM infrastructure. Its runaway success today is largely due to the fact that it lies at the core of access rights compliance and enforcement initiatives. However, provisioning only goes so far in serving this purpose by managing attributes and group memberships across systems. Entitlement management offers a more complete picture by looking at how applications apply that use information in the context of their own security. It promises to unify the administration of user privileges with their enforcement in real time as an access management function. As entitlement management matures and gradually integrates with IAM, we will see this component become a key factor behind IAM investment, and it will draw IAM market revenues from the provisioning segment of the IAM market.

## SUPPLEMENTAL MATERIAL

### Online Resource

The underlying spreadsheets detailing the forecasts in Figures 4, 5, 6, and 7 are available online.

### Methodology

To build these forecasts, we used a bi-logistic growth curve methodology in which we projected the total number of companies worldwide that would adopt IAM technologies. We scored each of the nine significant IAM categories — directories, metadirectories, virtual directories, provisioning, E-SSO, Web SSO, federation, password management, and privileged user management — on a series of adoption factors to calculate market saturation and total takeover time. We then multiplied the number of companies by the average annual deal size of IAM deployments for each component. To calculate annual deal size, we drew on vendor-specific deal sizes reported during our expert interviews, and then calculated the difference in each deal size by IAM category.

Evalueserve fielded telephone-based interviews with vendors and contributed to the development of the global forecast model. We used the following sources for the total number of enterprise and midmarket companies worldwide: the US Census Bureau, Eurostat New Cronos, and OneSource Information Services.

### Companies Interviewed For This Document

BMC Software
CA
Citrix Systems
Cyber-Ark Software
Hewlett-Packard
IBM
Mycroft/Talisen
Novell
Oracle
Passlogix
Sun Microsystems
Symark Software

## ENDNOTES

[1] Identity management is not any single product but an architectural framework for maintaining a person's complete set of identity information spanning multiple business contexts. Identity management unifies a person's disparate identity data to improve data consistency, data accuracy, and data and systems security in an efficient manner. Identity management requires both the integration of technologies like directories, single sign-on (SSO), provisioning, and delegated administration as well as coordination with the business processes surrounding the management of user information, access rights, and related policies. See the September 18, 2002, "Identity Management Architecture" report.

[2] Smaller enterprises (those with 1,000 to 5,000 employees) are an underserved market when it comes to user account provisioning. They are large enough to benefit from the efficiencies and controls that the technology provides, but they are not large enough to be able to justify the customization and integration efforts so often associated with provisioning. Success is attainable, and it comes from a keen focus on project scope. Right-size your provisioning project by securing the appropriate level of organizational support, spending enough time on business process redesign and role design, and consolidating user repositories at every stage. This will ensure that you realize your expected return on investment more quickly. See the August 20, 2007, "User Account Provisioning For The Midmarket" report.

[3] The integration of enterprise physical security controls and management regimes with enterprise IT security architectures is a nascent trend that has been forecast as imminent for several years. But despite the clear benefits to be gained from increased overall enterprise security risk management, the convergence trend is sluggish in taking hold among enterprises. Lack of clear exemplar converged architectures and a dearth of rich convergence-oriented vendor offerings are part of the reason. But the federal government's HSPD-12 initiative and key recent vendor announcements suggest that the convergence trend might finally be gaining some momentum. See the August 17, 2007, "Trends 2007: Physical And Logical Security Convergence" report.

FORRESTER®

Making Leaders Successful Every Day


**Headquarters**

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com


**Research and Sales Offices**

Australia
Brazil
Canada
Denmark
France
Germany
Hong Kong
India
Israel
Japan
Korea
The Netherlands
Switzerland
United Kingdom
United States

*For a complete list of worldwide locations, visit www.forrester.com/about.*



Forrester Research, Inc. (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. For more than 24 years, Forrester has been making leaders successful every day through its proprietary research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.

FORRESTER®