

February 6, 2009

Market Overview: Enterprise Role Management

by Andras Cser
for Security & Risk Professionals



February 6, 2009

Market Overview: Enterprise Role Management

Access Recertification And Role Management Converge, Integrate With Provisioning

by **Andras Cser**

with Simon Yates and Allison Herald

EXECUTIVE SUMMARY

Enterprise role management, role mining, and access recertification help enterprises with maintaining segregation of duties, keeping up with regulatory compliance requirements, and automating role-based provisioning to enterprise applications — even through difficult economic times. Forrester estimates that the 2008 enterprise role management market is at \$70 million, with a conservative estimate of annual growth rate of 70% to 90%. Key differentiating factors among products are: 1) the connector framework to endpoints; 2) risk scoring; and 3) management of rules defining roles. While consolidation is bound to happen in the intermediate to long term (12 months or more), today it's still a market of stack vendors and product specialists offering competing solutions that can operate independently or in collaboration with a user provisioning solution.

TABLE OF CONTENTS

- 2 **Identity Compliance Causes Pains For IT Security Professionals . . .**
- 3 **Why Role Management Matters**
- 4 **Trends Shaping The Enterprise Role Management Market**
- 4 **The Role Management Market Grows Phenomenally**
- 6 **Vendors Display Surprising Strengths Across The Board**
- 10 **Endpoint Connectors And Risk Scoring Are Key Differentiators**

RECOMMENDATIONS

- 13 **Look For Tried And True Vendor And System Integrator Partnerships**

WHAT IT MEANS

- 13 **More Market Consolidation Lies Ahead**
- 13 **DLP, Access Systems, And Event Monitoring Add Color To Roles**
- 14 **Supplemental Material**

NOTES & RESOURCES

Forrester interviewed 11 vendor and user companies, including Aveksa, BHOLD, IBM, Novell, Oracle, SailPoint Technologies, and Sun Microsystems.

Related Research Documents

- ["Best Practices: Enterprise Role Management"](#)
September 30, 2008
- ["Case Study: North American Financial Services Company Defines An RBAC Vision And Services"](#)
August 28, 2008
- ["The Forrester Wave™: Identity And Access Management, Q1 2008"](#)
March 14, 2008

IDENTITY COMPLIANCE CAUSES PAINS FOR IT SECURITY PROFESSIONALS . . .

Identity life-cycle management is an activity that IT organizations must undertake due to regulatory compliance, security, and IT administration effectiveness pressures. The challenges associated with identity life-cycle and access management are numerous. They include:

- **Checking and ensuring segregation of duties is difficult and error-prone to implement.** Like most other IT organizations, you probably have basic, manual methods to ensure that users don't get conflicting rights within an application but no way to detect conflicts between entitlements across applications.
- **Access recertification is a must, but preparation is costly.** Applications containing sensitive information need to be audited for compliance. Auditors want to know such information as how users gained access and why, who approved their access and when, and how long they have had access. Repeatedly answering these questions using manually generated and reconciled spreadsheets is time-consuming and expensive.
- **The number of controlled applications is growing constantly.** More and more applications are thrown at IT security administrators: They need to check segregation of duties, perform second-level approvals, and in some organizations manually add, change, or disable users in these applications.

. . . And The Current Economic Climate Is Making It Worse

As if that wasn't bad enough, the current economic climate means that you have to manage access and identity more closely than ever because:

- **You will probably use more temporary workers.** Temporary workers save on labor costs and increase flexibility during tough times, but their high turnover rate requires more administration and more careful identity verification. Keeping track of who has access to what and for how long is not easy.
- **Terminated employees need to be deprovisioned quickly.** Whether the account termination of separated workers is automatic or manual, it needs to happen quickly. Nobody wants ex-employees — or current employees who knew their passwords — to continue to access sensitive systems.
- **Reorganizations and rationalization heavily impact resource-strapped IT administration.** Since pure IT administration is often viewed as an activity with limited value, organizations tend to cut IT operations and administrator staff first. This leads to extended deprovisioning times. One company that Forrester spoke with indicated that it often takes up to 90 days to deprovision a terminated user from all user repositories.

WHY ROLE MANAGEMENT MATTERS

With the uncertainty that the current economic downturn brings, you need to be able to provision and deprovision employee and contractor access more accurately and with less IT administrative overhead. Enterprise role management can help. Forrester defines enterprise role management as consisting of the following sub-areas:

1) Role mining: the automated and widespread discovery of application-level entitlement; 2) attestation: the automated and workflow-driven access recertification of the user population; 3) role management: the grouping, management, and periodic recertification of application-level entitlements into enterprise (business) roles; and 4) provisioning integration: integration of the above functionality areas with user account provisioning solutions.

Forrester's interviews and inquiries indicate that enterprises implement enterprise role management because:

- **Roles allow easier and quicker segregation of duties.** A common audit finding is users who have conflicting access rights and entitlements. An example is a clerk working in the finance department who has acquired access to both the accounts receivable and accounts payable parts of an enterprise resource planning (ERP) system. These entitlements allow the clerk to single-handedly create and pay a purchase order to anyone — violating segregation of duties policies. Detecting these conflicting entitlements on a per-user basis is difficult and time-consuming. If an enterprise job role defines all the entitlements a user should have to perform his or her job, then segregation of duties becomes much easier. It boils down to checking only roles against each other and making sure that each role contains nonconflicting privileges. This is especially important when users transfer within the organization.
- **Access recertification is automatic and meets compliance requirements.** Since most users belong to one or more enterprise roles, their access recertification is almost automatic. Only access exceptions need to be approved by application owners and managers. There is no need for the IT security department to mine and report individual users' access rights, which saves money and time.
- **Workforce life-cycle management can be automated much more easily.** When users join, transfer within, or leave the organization, the bulk of their access is simply determined by their attributes — the organization they work in, their department code, or their job title — in an authoritative data source, which is often an HR or contractor database. Using rules, the enterprise role management system then translates these entitlement and access combinations into enterprise job roles.

TRENDS SHAPING THE ENTERPRISE ROLE MANAGEMENT MARKET

Organizations hit by audit findings usually want to get a head start on solving the problem by deploying access recertification. Access recertification allows you to gain an understanding of who has access to what and why. If you're defining segregation of duties — or preventing segregation of duty violations — you usually start by mining entitlements and managing them as groups of enterprise roles. Organizations trying to save expenses when granting, modifying, and revoking access automatically, with minimal manual processing, usually opt to introduce user account provisioning first.

No matter where you start, however, you will soon realize that the three aspects of role-based access control — role mining, access recertification, and role management — quickly form an iterative cycle. You need something to tie them together. Forrester found that the following trends are shaping the role management market today:

- **Solutions should make it easy to represent complex and non-linear organizations.** Life would be simple if all organizations and access rights could be described by an organizational chart. In reality, people work in different organizational units but may also belong to a special project or a peer group. Managers sometimes don't know what applications their employees should have access to.
- **Business friendliness is a key requirement.** The companies that Forrester interviewed for this report noted that provisioning solutions are difficult to use. Policy design is convoluted and requires an IT administrator to translate policies into the provisioning solution. Since most provisioning solutions are used to manage IT roles, these packages don't provide a rich abstraction layer or glossary of business terms, where membership in an Active Directory group "finadm29," for example, means that the user can approve bonuses. With the spreading use of access recertification solutions by line managers and business representatives, hiding cryptic IT resource names with business-friendly definitions is becoming the norm.
- **Role management and workflow support is a must if you don't use provisioning.** Even traditional access recertification vendors like Aveksa and SailPoint Technologies have added support for role definitions and workflows. If you don't have a full identity and access management (IAM) provisioning product, this allows you to get started with enterprise role management definitions and workflow-driven access recertification.

THE ROLE MANAGEMENT MARKET GROWS PHENOMENALLY

The market of enterprise role management products is fairly new and consists of both established IAM stack vendors (mainly through acquisitions) and point product specialist players. Forrester estimated the market size and vendors' market shares based on average deal sizes, growth of revenue, the number of new customers, and the number of customers that the vendors have in production:

- Conservative estimate of the market is \$70 million per year, with high-double-digit growth.** The market growth indicates organizations’ appetite to understand and manage access fundamentally differently and more efficiently. Based on the number of existing and new customers and average deal sizes, Forrester’s estimate for the 2008 enterprise role management market is \$70 million, with growth rates of 70% to 90%.¹ Based on client interest, Forrester expects double-digit percentage growth to continue into 2009 (see Figure 1).
- Vendors with integrated role management portfolios lead.** While IAM stack vendors are gaining ground with integrated product offerings, product specialists are following closely behind with highly responsive product teams and widespread integration with existing provisioning solutions. This underscores that organizations are looking for integrated product portfolios to integrate user account provisioning with enterprise role management and access control (see Figure 2).
- Large user bases and numbers of entitlements don’t necessarily require large vendors.** Aveksa, Eurekify, and SailPoint have been able to help large enterprises clean up entitlements, attesting to the power of artificial intelligence and automation in their solution (see Figure 3).

Figure 1 Main Indicators Of The Enterprise Role Management Market

Estimated total market size 2008 (licenses only, excluding services revenues)	\$70 million/year
Year-over-year growth of the market in 2008 compared with 2007	70%-90% (conservative estimate)
Geography focus	Tier 1: North America Tier 2: EMEA
Top verticals	Tier 1: Financial services, healthcare, public sector Tier 2: Manufacturing, telecommunications Tier 3: Utilities, retail
Average deal size	\$200,000-\$300,000

46469

Source: Forrester Research, Inc.

Figure 2 Enterprise Role Management Market Player Rankings

Estimated total market share tiers 2008* † (licenses only, excluding services revenues)	Tier 1: Sun Microsystems Tier 2: Aveksa, CA/Eurekify‡, IBM§, Novell, Oracle Tier 3: BHOLD, Courion, SailPoint Technologies
Which vendor do vendors and customers see most frequently in competitive situations?***	Tier 1: CA/Eurekify, Sun Microsystems Tier 2: Aveksa, Oracle, SailPoint Technologies Tier 3: BHOLD, Courion, IBM, Novell
Number of customers in production* †	Tier 1: BHOLD, CA/Eurekify, Novell, Sun Tier 2: Aveksa, Oracle Tier 3: Courion, SailPoint Technologies

*IBM did not disclose the number of role management specific customers in production, and because of this was omitted from the market share ranking.

† Companies within one tier are ordered alphabetically and not based on revenues.

‡ CA acquired Eurekify after September 30, 2008. For this survey, Forrester evaluated the Eurekify offering.

§ IBM's market share is estimated excluding purely TIM 5.0 role management deployments.

***Companies within one tier are ordered alphabetically and not based on revenues.

46469

Source: Forrester Research, Inc.

Figure 3 Vendors In Large Enterprise Role Management Deployments

Largest number of users whose entitlements are managed	Tier 1: Sun Microsystems Tier 2: SailPoint Technologies, Aveksa, CA/Eurekify, BHOLD, Novell Tier 3: Oracle, Courion, IBM
Largest number of entitlements mined across all connected systems	1. Aveksa 2. BHOLD 3. Oracle 4. SailPoint 5. Eurekify

46469

Source: Forrester Research, Inc.

VENDORS DISPLAY SURPRISING STRENGTHS ACROSS THE BOARD

The enterprise role management market is fairly new, and its players approach the problem from different angles. Forrester believes that what will eventually happen in the market is the larger IAM stack solution providers will acquire most of the smaller, specialist vendors. However, today it's still a market of full IAM solution providers and smaller product specialists offering competing solutions:

- **Aveksa covers over 253 million entitlements.** Aveksa started as an access recertification/role mining company, and then moved toward role management, user access request management, and workflow. The Aveksa Access Governance Platform consists of Aveksa Compliance Manager — which automates the monitoring, certification, and remediation of entitlements — and Aveksa Role Manager — which enables role discovery, modeling, analytics, and maintenance. Aveksa has a role

analytics engine and threshold capabilities to suggest key role management targets, the appropriate users and entitlements that should be in a role. Aveksa's dynamic collector framework can benefit those organizations that don't have provisioning systems implemented but want to monitor endpoints to ensure continuous identity compliance. Aveksa's largest enterprise implementation covers 253 million entitlements at a major North American financial services company. As of September 30, 2008, Aveksa had 12 production customers, with 17 prospects added in the 12-month period ending the same day. Forrester believes that Aveksa's solution is comprehensive in terms of access recertification and role management but remains concerned about long-term viability of the company as a standalone entity in the global world of integrated offerings.

- **BHOLD approaches from the centralized, dynamic role management perspective.** BHOLD is a privately funded, major player in Europe; its EAM solution has unique segregation of critical versus noncritical authorizations for onboarding applications and organizations in role management and avoiding role overgrowth by using parametric roles.² The product represents complex organizations using its "management dimensions" model, and provides a flexible model for dealing with out-of-role entitlements as exceptions. Its pricing model offers a convenient solution for those customers with lots of monitored systems, since the solution's price is not dependent on endpoints but is based on the number of security administrators. On September 30, 2008, BHOLD had 35 production customers and added eight customers in the 12-month period ending the same day. The majority of BHOLD's customers are European. The company is based in the Netherlands, which makes it a difficult-to-support vendor choice for North American organizations.
- **Courion provides a full suite of role management products integrated with provisioning.** Courion's roots go back to password synchronization and provisioning for small and medium-size businesses (SMBs), but recently the company has won large requests for proposals (RFPs) that mark its entry into the enterprise IAM market. RoleCourier, which is fully integrated with Courion's provisioning and compliance solutions, provides role mining (bottom up), role definition (top down), and role life-cycle management. The product uses its connector framework to collect ERP entitlements, which is a benefit to organizations that already use its provisioning solution. For full functionality, you will need to buy the entire suite. For example, excessive entitlements are discovered in the ComplianceCourier access recertifications product and are remediated in the AccountCourier provisioning product. However, "what-if" situations are modeled in the RoleCourier role management product. Customers looking for complete stacks will rely on Courion's partnership with EMC to include RSA Security ClearTrust as the access management platform. As of September 30, 2008, Courion had seven RoleCourier production customers and added a whopping 30 new customers in the 12-month period ending the same day.

- **CA strengthens its role portfolio with Eurekify acquisition.** CA Identity Manager has had support for managing provisioning roles for some time now, but these roles were primarily meant for managing application-specific IT roles rather than business job roles. Now, with CA's acquisition of the Eurekify Enterprise Role & Compliance Manager (ERCM) platform, CA can offer an IAM suite complete with a full offering of role mining and access recertification features. Eurekify's artificial intelligence-driven account correlation and heuristic role definition have been pioneering automation in role discovery. The tool uses analytics, including pattern recognition, not only to detect roles overgrowth, but also to propose pruning and other optimizations. For IT Infrastructure Library (ITIL) and process aficionados, the product can generate responsibilities/accountabilities/contribution/information (RACI) charts — a great feature for enterprises looking to get business users to at least partially own the role management process. ERCM cannot pull changes automatically from endpoints, as connected systems need to call Eurekify's Web services to keep the role management apprised of entitlement changes in connected endpoints. Although the product supports Java 2 Enterprise Edition (J2EE)-based administration, its full set of features is currently only available through a Windows32 graphical user interface (GUI), which can be a limiting factor for large-scale deployments. CA will have a lot of work to do to reconcile Eurekify's policy management, user interface, and functionality with the CA Identity Manager framework. Eurekify reported 100% revenue growth in the 12-month period ending September 30, 2008.
- **IBM uses entitlement management to capture roles.** Forrester includes IBM in this report, because IBM partners with Aveksa, SailPoint Technologies, and SecureIT for enterprise role management. IBM's Tivoli Identity Manager (TIM) has been providing significant and pioneering role management capabilities for a long time, for a great number of production customers, and IBM's TIM solution's acceptance has increased in the past nine months. IBM approaches enterprise role management from the entitlement definition and management perspective. Tivoli Security Policy Manager — although still in its infancy — will provide a holistic framework for integrating roles and fine-grained entitlements. While IBM solutions have been notoriously difficult to implement, this seems to be changing with the ease of integration of roles into TIM. IBM TIM also adds a unique dimension to IAM with the integration of role management with unstructured file management and managed file transfer. IBM could clearly benefit from acquiring a standalone role management specialist vendor like SecureIT or SailPoint Technologies.
- **Novell broadens its governance, risk, and compliance (GRC) offering with enterprise roles.** Novell developed the Novell Roles Based Provisioning Module as part of the Novell Compliance Management Platform (CMP). CMP is a business-level integration of provisioning, access, roles, and security information and event management (SIEM), based on common use cases with out-of-the-box interoperability. Novell's partnership with Aveksa adds role mining through the Novell Access Governance Suite. Novell supports Standard Provisioning Markup Language

(SPML) for role definitions. However, detailed role design happens via the Designer non-Web, client desktop user interface, which then loads policies into Novell Identity Manager, the central user account provisioning engine. Although the product does have a Web-based user interface (Identity Manager User Application), codification of policies could be an issue for large organizations that require support for distributed management. Novell supports role criticality and integrates IAM with its Sentinel SIEM solution, ZenWorks DLP endpoint, and Novell Storage Manager. Interviewees indicated that, typically, those organizations choose Novell's Roles Based Provisioning Module, where the Novell already was incumbent with its Identity Manager platform.

- **Oracle's holistic solutions project the most complete vision of role management.** Oracle Role Manager (ORM) automatically identifies users with excessive entitlements for cleanup, while integration with Oracle Identity Manager (OIM) automates the cleanup process across the connected endpoints. ORM's multidimensional organization (polyarchy) support allows administrators to define ad hoc workgroups and role assignments quickly. ORM's integration with Oracle Entitlement Server, entitlement management based partially on the BEA Aqualogic Enterprise Security (ALES) product acquisition, clearly signals that discovering, mining, managing, and enforcing entitlements constitute a tightly coupled process. Minor solution shortcomings include the following: 1) detecting out-of-band, unmanaged changes to entitlements in endpoints requires running the OIM reconciliation process — an inconvenience for ORM-only customers, and 2) administrators face a challenge in defining workflows — for the role management process, ORM uses business process execution language (BPEL), and OIM uses its own legacy workflow (Oracle plans to use BPEL for OIM's workflow in a later release). Of all the vendors, Oracle has implemented the largest number of enterprise roles (more than 10,000).
- **SailPoint Technologies forcefully enters the market during 2008.** SailPoint Technologies approached the role management market from the access recertification and role mining side, and added role management and workflow capabilities in late 2007. The IdentityIQ product represents business terms in its user interface and can monitor not only normal user but also privileged user and system administrator activity. Application and organization onboarding, role prioritization, and cleanup of excessive entitlements are aided by the product's advanced risk model. It also provides outstanding support for avoiding role erosion and cleaning up stale roles during access recertification. Of all the vendors, SailPoint Technologies reported the capability to manage the largest number of rules for role definition. Forrester remains concerned about long-term viability of the company as a standalone entity in the global world of integrated offerings.
- **Sun Microsystems is estimated to have the largest pure role management market share.** Sun Role Manager product is based on the RBACx product from the VAAU acquisition. Although initially offered as a consulting tool only, it has been widely used by system integrators and large enterprises for role mining and defining enterprise roles. Its flexible N levels of

entitlement hierarchy abstraction and explicit support for continuous compliance make it a robust candidate for managing role life cycles effectively. Of the vendors covered, Sun reported the highest number of managed users: 1.1 million people at a large financial services company. Sun's open source strategy on the access management side has increased 30%, but the business model still leaves Sun Role Manager product revenues vulnerable to a Sun's future opening of Sun Role Manager (SRM) code. On September 30, 2008 the product had 42 customers in production, and Sun added 26 new customers between October 1, 2007 and September 30, 2008. Sun's pure role management licensing revenues grew 112% in the same time period.

ENDPOINT CONNECTORS AND RISK SCORING ARE KEY DIFFERENTIATORS

All products, with the exception of IBM's TIM, support role mining, role management, role versioning, compliance reporting, definition, and enforcement of segregation of duties out-of-the-box. All solutions provide robust access recertification from the application owner's view, role owner's view, and manager's view. They uniformly provide GUI dashboards and detailed reports. Some level of help desk integration (BMC Remedy Service Management) is included with all products, and all products can call Web services. Distinguishing features are endpoint connector frameworks, dynamic risk assignment and management, Web user interface support for rule definitions, and Web services exposure (see Figure 4).

Figure 4 Enterprise Role Management Product Feature Comparisons

	<i>Endpoint connectivity</i>	<i>Solution runs on . . .</i>	<i>ERP system support</i>	<i>Automated entitlements cleanup</i>	<i>Dynamic access log monitoring</i>	<i>Organization representation</i>	<i>Risk assignment</i>
Aveksa	Own collectors	Linux, AIX, Tomcat, WebSphere	SAP, Oracle	Average	None	Full, unified	Automatic
BHOLD	CSV reader	Windows only	No special support	Average	Requires customization	Full	Manual
Courion	Own provisioning connectors	Windows only	Using own connectors	Average	Customization via connectors	Basic, hierarchy only	Manual
CA/Eurekify	No own connector framework	Windows only, some GUI on WebSphere, JBoss	SAP roles, Oracle, Great Plains, MFG Pro	Above average	None	Below average	Manual
IBM	TIM and SIEM connectors	Unix, Linux, Windows, z/OS	SAP, Oracle, Siebel, PeopleSoft	Average	TSIEM integration	Customization	Not available OOTB
Novell	Novell IDM connectors	Linux, Unix, Solaris, Jboss, WebSphere, WebLogic	Native support for Oracle business applications	Average	Sentinel/ Compliance Management Platform	Above average	Manual
Oracle	CSV flat file feed	WebLogic, WebSphere, Linux, Windows	Uses OIM integration	Above average	Access logs for dataset mining	Above average	Manual
SailPoint Technologies	Own connectors	Windows, Linux, Tomcat, WebSphere, WebLogic	Java-based read only connector	Above average	Via Activity Monitoring	Average	Automatic
Sun Microsystems	Flat file, CSV, ETL support	Any J2EE container platform (Windows, Unix, OS/400)	Requires customized ETL and XML	Above average	None	Average	Manual

46469

Source: Forrester Research, Inc.

Figure 4 Enterprise Role Management Product Feature Comparisons (Cont.)

	<i>Nested role definitions</i>	<i>Rule mgmt. in Web GUI</i>	<i>DLP solution integration</i>	<i>Reporting package</i>	<i>OOTB provisioning system integration</i>	<i>WSDL-based Web services exposure</i>
Aveksa	Yes	Yes	SIEM monitoring	Jasper	CA IM, IBM TIM, Novell IDM, Sun IDM, Oracle (planned)	Partial
BHOLD	Yes	Yes	None	JasperReports	CA IM, IBM TIM, Novell IDM, Sun IDM (planned)	Full
Courion	No	No, but planned	RSA enVision	SQL reporter tool only	Courion Enterprise Provisioning Suite	No, but planned
CA/Eurekify	Yes, also in role mining	Yes	None	BIRT	BMC, CA IM, IBM TIM, Novell IDM, Beta Systems, Hitachi ID, OIM (partial)	Full
IBM	SecureIT Role Manager	No	None	CrystalReports, Tivoli Common Reporting	TIM	Partial
Novell	Yes	No, Designer	ZENworks Endpoint Security integration	Jasper, CrystalReports	Novel IDM	Partial
Oracle	Yes, also in role mining	No, XML only	Simple OES integration planned	Oracle BI publisher	OIM	No, but planned
SailPoint Technologies	Yes	Yes	None	CSV export only	Sun IDM, TIM, Oracle IDM, Novell IDM	Partial
Sun Microsystems	Yes	Yes	None	SQL reporter tool only	Sun IDM, OIM, CA IM, TIM	Full

46469

Source: Forrester Research, Inc.

RECOMMENDATIONS

LOOK FOR TRIED AND TRUE VENDOR AND SYSTEM INTEGRATOR PARTNERSHIPS

Defining enterprise roles, even with automated mining, is not easy. In addition to following best practices, those users that selected a vendor and their system integrator (SI) partner with vertically relevant, recent implementation references, were able to significantly reduce implementation time.³ Experienced practitioners know how to set sensitivities and thresholds in the role mining application, and provide valuable business process definition, leading to a sustainable role structure. Automation of role mapping is not everything: You will still have to work one-on-one with your business representatives, gain their support, and implement a carefully phased role implementation process.

WHAT IT MEANS

MORE MARKET CONSOLIDATION LIES AHEAD

Sun's VAAU; Oracle's Bridgestream; CA's Eurekaify acquisitions; Novell's partnership with Aveksa; IBM partnering with SecureIT; and Courion's organic addition of RoleCourier, all point toward user account provisioning subsuming role mining, management, and access recertification. Forrester expects the acquisition wave to continue. User account provisioning is extended into business application platforms: Oracle Shared Services for Identity (SSI) is the first major step in that direction.⁴ Many organizations use IAM as their first entry into the governance, risk, and compliance space: IAM integration with GRC systems and business is thus becoming key for organizations wanting to implement a comprehensive IAM portfolio. This will foster tighter integration among GRC suites, business process modeling (BPM) tools, and IAM stacks, making policy maintenance much more seamless.

DLP, ACCESS SYSTEMS, AND EVENT MONITORING ADD COLOR TO ROLES

Role mining and engineering based on static entitlement data only shows the intended, but not the actual, view of access in the organization. Products increasingly add capabilities to monitor access control (Web single sign-on, desktop single sign-on, physical access, etc.) systems and allow this information to be continually updated and improve the role structure. Data leak prevention (DLP) integration, combining the data life-cycle management with the identity life-cycle management, will help solve security concerns of many organizations in a systemic way.

SUPPLEMENTAL MATERIAL

Companies Interviewed For This Document

Aveksa	Novell
BHOLD	Oracle
CA/Eurekify	SailPoint Technologies
Courion	Sun Microsystems
IBM	

ENDNOTES

- ¹ Information in this section is based on vendors' responses relating to their business and products as of September 30, 2008.
- ² Enterprise role management is not a project but a process. It only has a beginning, not an end, and if the organization wants to gain value from enterprise roles it needs to use a closed-loop process. This will ensure that roles reflect the current business situation and requirements, which will boost confidence among business and executive stakeholders. Forrester learned that enterprises iterate at least twice through a role design cycle before they can build a solid foundation for role-based access control (RBAC). A North American financial services company found that one full iteration cycle through a closed loop takes six to 12 months. They also found that to prove business value quickly, they needed to start with a small scope and extend it carefully. See the September 30, 2008, "[Best Practices: Enterprise Role Management](#)" report.
- ³ Enterprise role management plays a central role in efficiently managing access rights and enforcing access policies such as segregation of duties (SoD). The processes and tools related to role management consist of role mining and design, recertification, and access recertification. Forrester's IT end user interviews revealed that successful organizations implement and maintain enterprise roles by: 1) establishing a closed-loop process that covers all strategy, people, process, and technology aspects of role management; 2) leveraging existing access information and repositories for role definitions; and 3) targeting simple areas that yield high return, such as where there is high employee turnover or where the workforce performs common and repetitive tasks requiring access to a limited number of applications and application features. Next practices include: 1) feeding access log information to the role management system to ensure that role definitions remain up-to-date and reflect how applications are being used; 2) using entitlement management solutions to enforce fine-grained access policies tied to enterprise roles; and 3) extending role definitions to identify federation partners. See the September 30, 2008, "[Best Practices: Enterprise Role Management](#)," report and see the August 28, 2008, "[Case Study: North American Financial Services Company Defines An RBAC Vision And Services](#)" report.
- ⁴ Oracle's SSI will provide a future framework, interfaces, and applications (based on Oracle Identity Manager) to manage user life cycles in business applications.

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

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

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com.

We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, consumer insight, consulting, events, and peer-to-peer executive programs. For more than 25 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.