MarketScope for Enterprise Single Sign-On

Gartner RAS Core Research Note G00170568, Gregg Kreizman, 15 September 2009

The ESSO market has matured in 2009, with market leaders accelerating their growth at the expense of smaller players. ESSO is still a valid choice for enterprises with users who must manage an unacceptable number of passwords for two or more years.

WHAT YOU NEED TO KNOW

The enterprise single sign-on (ESSO) market has matured in 2009. Primary factors driving ESSO implementations are high password-related help desk costs and the need for shared workstation support. However, improved user convenience is the most deeply seated need. Enterprises turn to ESSO tools when users must manage a sustained, unacceptable number of user IDs and passwords for at least the next two years, despite attempts to reduce this complexity with other reduced sign-on tools and techniques.

There have been no major market acquisitions in 2009, although there were some packaging and OEM relationships that changed. Market leaders continued to outpace other vendors in new sales.

The trend to marginally improve product features and effectiveness has continued in 2009. Vendors that initially lacked competitors' distinguishing product features are now incorporating them, resulting in less feature differentiation. Now, vendors are separated more by their relative staying power in the market.

New rich interface applications (RIAs) are the latest battlefront for ESSO tool vendors to prove target system integration ease and effectiveness. Enterprises considering adoption should give special attention to applications with Flash, Java and mainframe terminal interfaces, and should require vendors to demonstrate an ESSO product's efficacy with these applications before purchasing.

MARKETSCOPE

In 2009, the "Magic Quadrant for Enterprise Single Sign-On" has been replaced by the ESSO MarketScope to reflect this market's maturity and the reduced criteria set that now differentiates vendors and products in the market. MarketScopes have a more coarse-grained rating system than Magic Quadrants do. Clients should not base product selection or shortlist decisions only on the basis of vendor ratings. We encourage clients to read the vendor comments in this research, to contact us with any questions or concerns, and to discuss enterprise-specific issues. Clients can also take advantage of "Peer Connect" to search for other Gartner clients that have implemented ESSO and are willing to speak with your organization.

Gartner

Enterprises continue to make tactical investments in ESSO to resolve the problem of users having too many passwords, with no relief in sight for the next two to three years. Client interest in leveraging Active Directory and using integrated Windows authentication have increased again in 2009, and using this method to achieve reduced or single sign-on is clearly strategic for many enterprises. However, other methods are needed for applications that cannot be integrated with Active Directory.

We typically see one or more types of password reduction initiatives – often being performed in combination – in our clients' organizations, and these initiatives can help reduce password management burdens on users and support organizations:

- **Harmonized and simplified password policies:** No automation tools are used here. The enterprise simply chooses to create a password formation rule policy and change frequently policy that are the same for all in-scope target systems. These can provide only minor benefits by potentially making password creation and change processes familiar to users.

- **Password management:** This includes self-service password reset (SSPR) or synchronization. SSPR lets users "get out of jail" and reset passwords when they forget them, and when they may be locked out of their accounts. This can reduce help desk calls; however, by itself, SSPR does not reduce the number of passwords that users have to contend with, unless users choose and maintain the same password for each target themselves. Password synchronization can reduce the number of passwords that a user must remember for the affected target systems to one. However, the password formation rules and password change frequency can only be as stringent as the target system with the weakest capability to meet the policy, because these passwords must be synchronized. Systems with weak password formation and change capabilities may be set aside and are not in scope for synchronization. With password management in place, user IDs and passwords must still be entered each time users access target systems.

- **Direct integration of alternative authentication with targets:** Passwords can be eliminated for any target system that has the authentication technology integrated.

- **Application authentication using Active Directory or Lightweight Directory Access Protocol (LDAP):** Here, the user ID and password are the same for any integrated application, although users must enter them each time they sign on. The target system's scope of this solution is limited to applications that can be integrated with LDAP. Many cannot.

- **Kerberos:** Microsoft adopted the Massachusetts-Institute-of-Technology-developed Kerberos network authentication protocol as the underlying technology for enabling authentication and SSO in Windows and Active-Directory-enabled applications. Application developers and commercial off-the-shelf products are increasingly taking advantage of the underlying Active Directory environment that's present in enterprises. Unix and Linux systems can also be integrated with Active Directory/Kerberos using a variety of methods, like Active Directory/Unix integration tools from vendors such as Quest Software, Centrify, Likewise Software and BeyondTrust (formerly Symark). Use of Kerberos is generally limited to internal, inside-the-firewall SSO.

- **Web SSO with Web access management (WAM):** These tools provide authentication, generally to Web applications only, although there are integration kits for no-Web applications. WAM tools also have limited user provisioning and coarse-grained authorization capabilities. In addition, WAM tools include federated SSO or serve as a platform for providing federated SSO as an add-on option. WAM tools are used inside the enterprise as an SSO integration tool for Web applications on disparate platforms, or as externally facing tools to enable external users to have SSO to enterprise applications.

- **Federated SSO:** This refers to the capability to provide users in one trust domain with SSO to applications in another domain – that is, to applications managed by another organization with its own identity infrastructure. This could be another part of the enterprise, a business partner, a business process outsourcing provider or a software-as-a-service (SaaS) application provider. Stand-alone federation tools, WAM tools and identity access management (IAM) SaaS gateways are all options to meet this need.

Any of these tools can reduce the problem space and the number of IDs and passwords to be managed.

Conversely, in many organizations, some legacy applications can't be retired within two to five years. IT organizations supporting business unit applications may not have the clout to require these business units to purchase new systems that fit the standard identity management and authentication architectures. In addition, merger-and-acquisition activity may introduce nonstandard systems. The compliance trend of stronger passwords on targets also can exacerbate support issues for passwords. Integrating new authentication methods directly with many disparate targets can be difficult, particularly with legacy mainframe applications.

Most enterprises' initial ESSO implementation times range from three to six months; this is the time it takes to integrate a planned set of applications (from 10 to 20) and to deploy to an initial set of users (hundreds to 2,000). It takes roughly two years to recoup the costs associated with the purchase and integration of ESSO products, and these costs may be soft – that is, associated with help desk labor savings that can't be monetized.

Some project needs can prolong implementation times, and, therefore, time to value. Applications that cannot easily be integrated through the ESSO tool's application profiling or scripting tools can add time to a project. Implementing authentication technologies for the first time, coincident with the ESSO project, can extend project times because endpoints may require hardware installation.

Implementing shared workstation support also can prolong a project. In clinical healthcare organizations, it is very important to make the workflow associated with shared workstation sign-on fast and efficient. Greater variation among shared workstation users, with the application set being used and more automation beyond sign-on (such as navigating applications to open specific patient records), can also add to project implementation times.

Enterprises must analyze the set of known and anticipated simplification initiatives, balance them against the competing complexity factors, and determine whether the results will provide an acceptable solution within a two- to three-year time frame. For example, if an Active Directory integration strategy can reduce the need for user IDs and passwords from six to three, then will that be sufficient? If not, then ESSO might be more strongly indicated.

Market Changes: The ESSO market has continued to mature in 2009. Most vendors with products that lacked core functionality have improved their products, and it has become more difficult for vendors to differentiate themselves based on product functions and features.

Most market leaders from 2008 have continued to enhance their customer bases, and have moved more aggressively into geographic markets that are outside their current territories. Niche vendors and challengers realized modest customer gains in 2008.

In 2008, Passlogix lost a major reseller in IBM when IBM acquired Encentuate. Over the course of the past year, IBM was able to retain the majority of customers that initially bought the rebranded Passlogix product, and we are seeing signs that many of these customers are converting to the product that IBM now manufactures. However, Passlogix retained a significant portion of these customers and has expanded its presence in the market with some very large deals. A portion of its success is due to having Oracle as a partner.

Citrix has ceased marketing Password Manager as a stand-alone product; instead, it is marketing SSO functionality as a feature set within its XenApp Platinum suite of products.

Novell has licensed the source code to SecureLogin from ActivIdentity, and it will now follow its own path for product enhancements.

Imprivata continued to gain customers at an impressive rate.

Gartner estimates that the total 2008 software revenue for the ESSO market was approximately $156 million, and grew at a rate of 10% over 2007.

Pricing: Advertised pricing has changed little in 2009, although good deals are available – spurred by prevalent economic conditions. Gartner has collected prices for different numerical ranges of purchased seats, and we also asked vendors to price two scenarios.

Scenario 1 was for a regional hospital that has four locations and requires operations to be automatically resumed/handled by another location when one location fails. The scenario included the following requirements:

- 1,000 users
- Active Directory
- Applications were Microsoft Exchange, SAP with an SAP graphical user interface, Lotus Notes, six additional thick-client Windows applications and six Web applications
- Shared kiosk/workstation support for 500 of the users
- Passive proximity card integration for all users
- The cost of any new authentication integration software that's required by the vendor's ESSO product, but not the cost of the technologies themselves
- Three years of product maintenance costs to be included

The average price for this scenario was $86,000.

Scenario 2 was for a manufacturing company in one location:

- 5,000 users
- Standard Web, Windows and terminal applications
- Remote access required for 1,000 of the users on unmanaged machines
- No new authentication methods or shared kiosks
- Three years of product maintenance

The average price for this scenario was $264,000.

The cost of new authentication technologies isn't included in these average figures, and can add $15 to $100 per user to implementation costs.

Integration Realities: ESSO products serve as a proxy between client devices and target systems. Target systems still maintain independent credential stores and will present unique sign-on prompts to users' client devices. ESSO products provide various mechanisms to sense sign-on, user ID, password and password change prompts for different target systems, and they broker the needed data to the targets.

Vendor capabilities with ease of target system integration have remained mostly consistent with the 2008 findings; however, the increased prevalence of RIAs, such as those using Flash, Silverlight or Ajax, may be increasingly problematic because these RIAs have different or nonexistent hooks for SSO automation. Based on references and client interactions, we found that these products can be integrated out of the box (with approximately 90% of their target systems) using the chosen product's automated discovery features. Most remaining applications can be integrated using the provided utilities, scripting or some customization.

Difficult-to-integrate applications add time to implementations, and products that require custom coding that is external to the ESSO product's native automation or scripting environment can add significant implementation time and costs. A few applications can't be integrated at all. More Java applications and RIAs are making their way into enterprises, and some vendors' products have difficulty recognizing sign-on and password change prompts when the interface provides nothing but graphical content for the ESSO product to analyze. Most vendors are having to enhance their products to improve Java application sign-on recognition.

Automated sign-on logic can fail when sign-on or password update prompts change with new releases of target applications or operating systems (OSs). For example, an ESSO product must rely on textual prompts for terminal, emulator-based applications, and will fail when this text changes. If mitigated after the fact, then administrators must retrain the ESSO product to recognize the new prompt. Therefore, when updating target systems, enterprises that adopt ESSO products must incorporate ESSO testing into the enterprise change management process.

Shared workstation support, and the addition of post-sign-on menu or transaction navigation, also can be complex, and extra time should be given to proofs of concept and pilot implementations to handle these scenarios.

Architectural Differences: All ESSO products provide similar core functionality. However, there are key architectural differentiators among products, as described below.

Creating Sign-On Automation: Every product provides a graphical wizard that helps administrators "train" the product to recognize various sign-on, password change and sign-off events. The wizards write scripts or XML parameter files that are input to the sign-on agent to drive automation. Well-designed, wizard-based administrative interfaces and sensing capabilities generally do a good job of making the automation integration task easy for administrators. These wizards tend to be easier to use than approaches that require script editing. However, wizards can lack flexibility in the product for difficult-to-integrate applications, and may force the administrator or integrator to make external calls to command-line scripts and other executable code. This may cause difficulties for the product's primary internal support staff.

Combined wizard-and-script approaches provide a common way to deal with difficult-to-integrate applications, and require only one method to learn, rather than having to know various integration methods. Before purchasing, potential customers conducting evaluations or proof-of-concept exercises should provide shortlisted vendors with a set of representative Windows, Web, Java, RIAs and legacy/terminal-based applications, and should demand that these vendors demonstrate the methodologies and efforts required to integrate the diverse application types.

Repository: The back-end repository that's used to hold objects (such as identity attributes, encrypted credentials, application profiles, administrative options and security policies) may be based on directories, databases, and, less commonly, file systems. Most products use directories and support Microsoft's Active Directory or various LDAP-based directories. Some products use relational database management systems (RDBMSs) to hold all or some objects, but may interface with directories to synchronize identity attributes. Potential customers should evaluate vendors' repositories of architectural choices against internal architectural standards.

Two-Tier vs. N-Tier Architecture: In a two-tier architecture, ESSO client agents and administrative client agents interact directly with the directory infrastructure. In an n-tier approach, ESSO products use a physical and logical middle-tier architecture to interact with clients and administrative agents; in addition, they broker interactions with an RDBMS or directory. Implementing a middle-tier architecture may provide ESSO vendors with a platform for the following additional features, relative to providers of two-tier architectures: the ability to limit access by workstation address, and the ability to force a sign-off from one workstation if a user walks away and signs onto another workstation (which is an issue with shared workstations in clinical care):

- Fine-grained administration and delegation
- Web interface for administration
- User-provisioning connectors

Some vendors' implementations of middle-tier architectures require the customer to implement needed resiliency on its own – for example, by using redundant server configurations. Customers that purchase ESSO products with middle-tier architectural components should implement these components redundantly with the chosen vendor's product, or with separately purchased products. Two-tier architectures inherit the fault-tolerance capability of the directory that's used to hold credentials and administrative information. However, some two-tier approaches require a directory schema extension to add administrative attributes or credential caches. Potential ESSO customers have expressed concerns about this, particularly in large organizations, because of potential directory failures or performance issues that can result from schema

extensions. In almost all cases, two-tier and n-tier architectures enable users' encrypted credential stores to be held locally on the workstation. This can provide temporary SSO access to local resources and available network resources, in case the directory or middle-tier repository is down.

New Authentication Integration: Vendors offer many choices for integrating alternative authentication methods, such as fingerprint biometric technologies, proximity badges, one-time password (OTP) tokens and smart cards. ESSO vendors use various integration methods, including their own toolkits, or toolkits provided by authentication vendors, and standards-based integration that uses OS-provided utilities and interfaces, such as for smart cards.

In 2009, we have again collected data regarding the use of alternative authentication with ESSO products. We estimate that, on average, 25% of all customers implementing ESSO augment with alternative authentication. This percentage is higher for customers of vendors that have authentication products in their portfolios, or have business roots in the authentication markets. This percentage is also higher in certain industries and geographies. Healthcare customers are increasingly deploying a combination of proximity cards and passwords for authentication to ESSO. European customers generally favor standard smart cards as an alternative authentication method.

Customers should require ESSO vendors to clearly articulate the techniques they use to integrate the selected authentication technology. In addition, vendors should be required to answer these key questions:

- Are integration software/drivers provided, or must they be purchased separately?
- How is a second authentication event implemented? Some customers require a second authentication event for sensitive target applications. Is it enabled simply by the administrator checking a box in an administrative tool, or does it require custom integration? Does the user interface ask for the secondary authentication in line with accessing the target system (best), or does it blank the screen and force the user interface back to the main Windows authentication prompt before proceeding to the application?
- Does alternative authentication integration require the Microsoft Graphical Identification and Authentication (GINA) dynamic link library to be replaced? Doing so can be problematic for some organizations because the library may be incompatible with a new version of Windows. The ESSO product may have to replace the GINA if an alternative authentication method is used for the initial Windows logon, or if additional functionality (such as SSPR) is built into the augmented GINA. Most often, however, the ESSO's GINA enhancements are implemented by "chaining" to the Microsoft GINA, and no replacement is required. However, there may be issues if the Microsoft GINA has already been replaced by an augmented GINA, such as Novell's.

Reporting: All vendors provide products that log key events to be used in auditing. These log entries only provide basic information about who has access to which applications, and about who accessed which applications and when. Vendors differ in whether they provide canned reporting functionality as part of the offering, or whether they rely on exporting log data to third-party reporting or system management tools. Enterprises that have an overarching IAM strategy with a central audit and reporting repository are less likely to be concerned with ESSO products that lack inherent reporting capabilities.

Market/Market Segment Description

ESSO products enable users to authenticate once to the product, and then to be subsequently and automatically authenticated to other target systems when they're accessed – almost always without modifications to the target systems. ESSO products provide this functionality for systems that use Windows, network, Web and terminal client interfaces. ESSO products also handle password change requests from target systems, and may support post-sign-on automation for additional tasks. ESSO is only one segment of the authentication-related marketplace within the broader IAM marketplace.

Inclusion and Exclusion Criteria

Vendors were rated in this MarketScope if they have considerable market share among Gartner clients, and have shipping products that have capabilities and attributes that:

- Enable users to sign in once and automatically be signed into secondary applications without requiring a second identification and authentication action
- Support target applications that require Windows (thick client), terminal emulator and Web client interfaces
- Are manufactured by the vendor, or are significantly modified versions of the products obtained through OEM relationships (the products aren't obtained without functional modification as part of reseller/partner agreements)
- Don't have password synchronization without SSO
- Don't provide Web SSO only
- Don't require bundling the vendors' authentication technologies only, and support various authentication methods (for example, OTP tokens, biometric methods and smart cards) from multiple third-party vendors

Vendors Added

No new vendors were added to the ratings in 2009.

The following vendors are noteworthy, but they weren't rated in this market study:

- **Hitachi ID Systems:** Hitachi ID's Login Manager and Password Manager combine to offer reduced sign-on with password synchronization. Login Manager automatically populates application login IDs and passwords for users in a way similar to ESSO products, but does not store passwords. Instead, passwords must be consolidated or synchronized for the SSO

component to function. Login Manager downloads a network provider after Windows login to provide the SSO capability. The advantage is that there is no local password wallet. The disadvantages are that application and OS passwords are the same on all target systems, which can be a security weakness, and the product does not support authentication methods other than user IDs and passwords.

- **Secude** has provided secure SSO solutions for SAP for several years. It has also specialized in smart-card-based ESSO for OS, Web and Windows applications. In 2007, Secude developed broader SSO functionality that works without smart cards. The latest version of SSO also supports Java applications without external calls to scripts or programs. Secude is working to address automating terminal emulation client access and Windows 7 support in its next release.

- **Softex** had its beginnings as a provider of basic input/output system and device driver software to PC manufacturers, and it has evolved authentication capabilities to provide SSO. OmniPass is its ESSO product's name. Softex's client (nonenterprise) ESSO has shipped with standard builds on some models of Fujitsu, Lenovo, Toshiba, Samsung, LG Electronics and Motion Computing computers. Its ESSO is full-featured. OmniPass also provides file and disk encryption. Softex has been building its client base for OmniPass in 2009.

Vendors Dropped

- **Citrix** stopped marketing Password Manager as a stand-alone product, and instead includes ESSO functionality in its XenApp Platinum suite.

- **MetaPass** was dropped because Gartner could not confirm a significant customer base.

Rating for Overall Market/Market Segment

Overall Market Rating: Positive

ESSO remains a requirement for many enterprises. Even though it is a much smaller market than WAM or user provisioning, ESSO has continued to grow during a down economy. Most vendors have participated in this growth. These factors contribute to our generally positive outlook for the next one to two years.

Vendor Product/Service Analysis

ActivIdentity

Strengths

- ActivIdentity is a long-standing vendor in the ESSO market, having produced or supported acquired products since 1991.

- ActivIdentity's pricing model remains favorable, relative to the market average. The company has continued its solid global coverage in sales and support, and it has several ActivIdentity SecureLogin Single Sign-On resellers in Europe and the U.S.

- ActivIdentity's combined wizard-and-script integration capabilities provide a common language to deal with difficult integration problems, rather than having to call external executables. In 2009, the ability to enable Java applications and Oracle Forms automation for SSO within the unified wizard was added.

- ActivIdentity SecureLogin Single Sign-On supports a solid variety of authentication mechanisms, with particular strengths in smart-token integration.

Figure 1. MarketScope for Enterprise Single Sign-On

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
ActivIdentity				x	
Avencis			x		
CA				x	
Evidian				x	
IBM					x
Imprivata				x	
i-Sprint Innovations			x		
Novell					x
Passlogix					x
Sentillion				x	

Source: Gartner (September 2009)

Evaluation Criteria

Table 1. Evaluation Criteria

Evaluation Criteria	Comment	Weighting
Offering (Product) Strategy	The ESSO product's top selling points, brand or industry, or geography specialization and generalization; the vendor's professional service capability; and the use of system integrators.	Standard
Vertical/Industry Strategy	The technology provider's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical industries. Weight given to a broad and deep client base in many industries, with healthcare, financial services, manufacturing and government being the most important.	Standard
Geographic Strategy	The technology provider's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, directly or through partners, channels and subsidiaries as appropriate for the geography and market.	Standard
Product/Service	The ESSO product's functionality, architecture, ease of integration, scalability, resiliency, breadth and quality of authentication support, administration and reporting, and shared workstation capability.	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	The workforce directed to develop, sell and service the solution; installed base; and historical and forward-looking financial results for the product segment. Ability to achieve competitive success, customer wins over competitors, changes in capabilities based on customer needs, and significance in ESSO milestones.	High
Sales Execution/Pricing	Pricing for the base ESSO product, and with options for different-size customer organizations, customer wins and seat sales.	Standard
Customer Experience	Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes how customers receive technical support or account support. This also can include ancillary tools, customer support programs (and the quality thereof), availability of user groups and service-level agreements. Customer experiences with products and services, as obtained through references and via other Gartner client-interaction channels, were very important. These interactions also helped in the evaluation of product/service capabilities.	High

Source: Gartner (September 2009)

- ActivIdentity has good cross-selling potential, and can leverage its authentication and credential management business for ESSO integration and sales. Conversely, ESSO helps drive other lines of business.

Cautions

- In 2009, ActivIdentity lost Novell as its OEM partner when Novell licensed the source code for ActivIdentity SecureLogin. Novell's sales were a solid source of revenue for ActivIdentity.

- ActivIdentity SecureLogin Single Sign-On supports various directories; however, it requires a directory schema extension. A separate instance of Microsoft Active Directory Lightweight Directory Services (AD LDS) could be an alternative. This caution is counterbalanced by ActivIdentity SecureLogin Single Sign-On's capability to be easily integrated with Active Directory, Novell eDirectory (via LDAP) and LDAP.

- ActivIdentity withdrew out-of-the-box support for shared workstation fast user switching. However, this can still be obtained through a professional service package.

- The majority of new ActivIdentity SecureLogin Single Sign-On sales have been to smaller customers. However, in 2009, the overall seat count on maintenance has dropped. ActivIdentity's recent financial statements suggest that its turnaround plan is working, and we are less pessimistic about the company's long-term viability.

Avencis

Strengths

- In 2009, Avencis has continued gaining customers, and at an increased rate, for its SSOX Single Sign-On software suite in its constrained and targeted European marketplace.

- SSOX pricing is highly competitive for small implementations, and the product offering bundles in self-service password reset, shared workstation support, and emergency access with question-and-answer identity verification when users' regular authentication technologies are unavailable.
- Avencis has excellent breadth of directory support and easy integration.
- SSOX supports a wide variety of vendors and types of authentication methods, and these methods are easily integrated with SSOX.
- SSOX features a solid reporting capability, delegated administration and the administrator-controlled ability for users to delegate their SSO access to others.

Cautions

- Avencis remains focused on sales in Europe, predominantly in France. Integration and sales partners are few. Although the company manages expenses well and remains profitable, SSOX is a poor choice for geographies outside Europe.
- Although SSOX is full-featured, it is Avencis' only product, thereby making it difficult to cross-leverage SSOX sales with other products to generate new business.
- Pricing for larger implementations is one of the highest among vendors in the market.

CA

Strengths

- CA Single Sign-On is part of the company's broader IAM suite. As with other vendors that offer identity and security products beyond ESSO, CA can leverage sales bidirectionally to upsell. CA has some very large ESSO installations, with one confirmed at 65,000 users.
- CA has a broad geographic range for selling and servicing its product. The company predominantly relies on its direct channel, but has large, worldwide system integrators as partners.
- CA Single Sign-On supports a wide variety of authentication technologies.
- The shared workstation functionality is very good and has the advanced features found in other strong products. These features include automated logoff, application closing and activation/deactivation based on the presence or absence of a smart token or proximity card.

Cautions

- CA didn't improve on its automation wizard in 2009; it still supports only Windows and Web applications. Terminal emulator and Java applications still require scripting in Tcl (Tool Command Language). CA provides customers with access to a large set of predefined application scripts. However, based on references and client feedback, CA Single Sign-On is stable when implemented, but, on average, it takes longer to implement than other solutions.
- CA has focused on developing its other more-lucrative IAM toolsets, and little has changed with the Single Sign-On product in 2009, except for enhancements such as Section 508 accessibility support for the U.S. federal market.
- Customers must pay for a "lite" version of CA's provisioning product to get SSPR added to Single Sign-On. SSPR is part of CA's Identity Lifecycle Management offering.

Evidian

Strengths

- Evidian maintains a strong presence and sales record in Europe, and has made inroads outside the continent with some gains in the U.S., where Evidian is supported by Quest Software as a reseller.
- Evidian Enterprise SSO has a capability that enables users to delegate SSO capabilities to other users (for example, when going on leave), while maintaining audit information that's linked to the user receiving the delegation.
- Authentication support is broad and well integrated with the core product, and plays well to the regional preference for smart card support.
- Evidian's product has very good out-of-the-box support for multiple directory products.

Cautions

- Despite its success, Evidian continues to face European competition from Passlogix, Imprivata, Novell and IBM.

i-Sprint Innovations

Strengths

- i-Sprint Innovations has been successful in selling its AccessMatrix Universal Sign-On (USO) to banks and other customers, predominantly in the Asia/Pacific region. In 2009, the company's customer base spread throughout that region, and more customers were picked up in Japan.
- USO is part of a larger access management and authentication portfolio that includes WAM and shared account password management.
- USO has a middle-tier architecture that provides granular administrative control, as well as good audit and reporting features favored by financial institutions. USO also supports various back-end directories.
- USO's middle-tier architecture can be hosted on various OS platforms, including IBM z/OS, Linux, Unix and Windows. USO also supports a variety of databases to hold identity attributes and security policy data.
- USO can segregate administrative duties, and optionally may require two different users to perform administrative functions, or require two users to log into particular target systems (which is analogous to requiring two keys to unlock a safe deposit box). This unique feature was developed for banking environments.

Cautions

- Although i-Sprint has a niche in financial services and some government customers, and its presence has spread to Japan, the company's customer base remains small, as are its seat counts at customer sites.

IBM

Strengths

- IBM has turned the corner with the assimilation of Encentuate's ESSO tool, which is now branded as IBM Tivoli Access Manager for Enterprise Single Sign-On (TAM ESSO). This product now has the worldwide distribution, integration and support channels that Encentuate lacked. IBM has successfully converted a large majority of customers from the formerly rebranded Passlogix product to IBM's own product. We believe that TAM ESSO will increasingly be more integrated with IBM's other access management offerings.
- Based on client and reference feedback, TAM ESSO has a high rate of out-of-the-box integration with target systems.
- TAM ESSO is the only product that can provide access to all types of applications through a Web browser, and without requiring the SSO client to be implemented or downloaded to the remote workstation.
- The IBM product set integrates with a good set of authentication options, and includes support for a unique product called iTag. This is a passive proximity/radio frequency ID reader with a tag that can be affixed to anything the user carries (often a physical ID or physical access control badge), and it can be used as a form of authentication for TAM ESSO.
- TAM ESSO has excellent shared workstation support and the capability to provide each user with a private desktop – not just the sharing of applications with a common desktop, as other vendors do.

Cautions

- IBM's retail pricing is some of the highest in the market. This may limit its solution's consideration beyond large enterprises, but clients should still investigate what discounts they may obtain before eliminating the solution based on retail price.

Imprivata

Strengths

- Imprivata continues making solid customer count gains on the strength of its reseller channels, its appliance-based approach and its ease of target system integration. Imprivata OneSign repeatedly stands out because of its capability to integrate easily with target systems and provide the needed sign-on, password changes and follow-on automation, while rarely requiring external command calls.
- OneSign has very good authentication integration, shared workstation capabilities and end-user workflow support.
- OneSign also includes a solid set of canned reports.
- Clients and references regularly report easy integration and implementation experiences.
- Imprivata sells a versatile authentication management server that uses the same platform as ESSO, and, therefore, it has easy upgrade and cross-sell opportunities. There is also a physical/logical integration product available that can correlate logical authentication events with physical access control events to make access decisions. For example, the product could be used to determine whether an employee has "badged in" using the building's physical access control system before allowing him or her to sign onto systems. We have not been able to confirm much uptake of this capability. However, it may be of interest to clients that want to leverage the combination of physical and logical access controls.

Cautions

- Despite its overall rapid customer growth and expansion into Europe, the Middle East and Africa, Imprivata is still venture-funded and not profitable (although it continues to be headed in that direction). We don't have any immediate concerns regarding Imprivata's viability, and we will monitor its progress.

- On average, Imprivata's implementations are still smaller than its competitors, and its largest customer has approximately 23,000 deployed users.

Novell

Strengths

- In 2009, Novell licensed the source code for SecureLogin from ActivIdentity. Novell also picked up key developer and sales personnel in 2009. Previously, Novell had been more of a value-added reseller of SecureLogin, although it created its own Novell Modular Authentication Service (NMAS) to support the integration of various third-party authentication for eDirectory customers. Novell also provides an iManager plug-in for SecureLogin that enables administrators to use a Web interface for portions of the administrative functionality, such as setting user and group policies to provide access to specific target systems. SecureLogin can use Microsoft Active Directory or Microsoft AD LDS (formerly known as ADAM) as a repository, and no Novell infrastructure is required. We believe that the new license agreement will lead to an even stronger product suite for Novell, which has a history of providing highly integrated IAM solutions.

- Novell has a global reseller channel, "follow the sun" support and consulting services to support implementation.

- Novell gained significant customer and seat count again in 2009.

- Novell's pricing is very attractive and one of the lowest in the market.

Cautions

- Novell SecureLogin supports multiple authentication methods using different integration techniques. The consistent handling of different authentication methods afforded by NMAS is only suitable when Novell eDirectory is used for authentication, and potentially in mixed eDirectory and Active Directory environments.

- SSPR requires the Novell Identity Manager and user application portal.

Passlogix

Strengths

- Passlogix has continued to outpace competitors with new customers, it has extended seat count, and it was able to wrest away some key accounts that had been IBM customers that bought the rebranded Passlogix product. Resellers, most notably Oracle, have contributed to this success.

- Passlogix has demonstrated that its product can scale. It has several very large implementations, and in 2009, it added more – some with more than 100,000 users.

- Passlogix's sign-on automation is wizard-based and parameter-based, so no scripts are used. Clients report that most applications can be easily integrated out of the box.

- Passlogix has an "on demand" functionality that enables remote users to download the client agent on demand and have the agent persist on the endpoint. This avoids a normal Windows system installation.

- Good shared workstation support comes with the add-on product, v-Go Session Manager. In addition, Passlogix supports integration with various provisioning products via its add-on product, v-Go Provisioning Manager.

- The company has cross-sell opportunities with its shared account password management product.

Cautions

- Some target systems can be difficult to integrate, will require additional time and may require code updates from Passlogix.

- Passlogix's retail pricing is some of the highest in the market; however, clients considering Passlogix should still ascertain the potential for discounts before eliminating the company based on retail price alone.

Sentillion

Strengths

- Sentillion has its roots and strengths in the demanding healthcare industry. The company has provisioning capabilities, strong context management and remote-access tools for ESSO. Sentillion's products are almost always on our healthcare clients' shortlists for consideration, and Sentillion's SSO tools have demonstrated scalability for large environments.

- Sentillion also has a very good project-oriented implementation methodology, as well as a fixed-price engagement for helping clients implement their ESSO products.

- Sentillion has gained solid new customers and seat count; in addition, it captured significant market share in 2008 and remains profitable in 2009. Sentillion is the only vendor in this research that's focused on one vertical industry and meets the eligibility criteria to be included herein.

- Shared workstation support is excellent and provides all required functionality demanded by clinical healthcare environments.

Cautions

- Sentillion's client base is limited exclusively to the healthcare industry and almost exclusively to North America. Sentillion sells its ESSO solutions to other markets through its network of channel partners. However, the company continues to face competition in the healthcare industry from the combined forces of CA, IBM, Imprivata, Novell and Passlogix.

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Gartner MarketScope Defined

Gartner's MarketScope provides specific guidance for users who are deploying, or have deployed, products or services. A Gartner MarketScope rating does not imply that the vendor meets all, few or none of the evaluation criteria. The Gartner MarketScope evaluation is based on a weighted evaluation of a vendor's products in comparison with the evaluation criteria. Consider Gartner's criteria as they apply to your specific requirements. Contact Gartner to discuss how this evaluation may affect your specific needs.

In the below table, the various ratings are defined:

MarketScope Rating Framework

Strong Positive

Is viewed as a provider of strategic products, services or solutions:

- *Customers:* Continue with planned investments.
- *Potential customers:* Consider this vendor a strong choice for strategic investments.

Positive

Demonstrates strength in specific areas, but execution in one or more areas may still be developing or inconsistent with other areas of performance:

- *Customers:* Continue planned investments.
- *Potential customers:* Consider this vendor a viable choice for strategic or tactical investments, while planning for known limitations.

Promising

Shows potential in specific areas; however, execution is inconsistent:

- *Customers:* Consider the short- and long-term impact of possible changes in status.
- *Potential customers:* Plan for and be aware of issues and opportunities related to the evolution and maturity of this vendor.

Caution

Faces challenges in one or more areas.

- *Customers:* Understand challenges in relevant areas, and develop contingency plans based on risk tolerance and possible business impact.
- *Potential customers:* Account for the vendor's challenges as part of due diligence.

Strong Negative

Has difficulty responding to problems in multiple areas.

- *Customers:* Execute risk mitigation plans and contingency options.
- *Potential customers:* Consider this vendor only for tactical investment with short-term, rapid payback.