MarketScope for Enterprise Single Sign-On

Gartner RAS Core Research Note G00206199, Gregg Kreizman, 7 September 2010

The enterprise single sign-on market continues to mature in 2010. A few vendors are dominating most of the new business. ESSO remains a valid choice for enterprises requiring automated sign-on of new and legacy application targets not enabled by other means.

WHAT YOU NEED TO KNOW

The business case for implementing enterprise single sign-on (ESSO) has solidified. Factors driving ESSO implementations are high password-related help desk costs and the need for shared workstation support in clinical environments. However, improved user convenience is usually the most deeply seated need, whether or not this need is openly articulated. 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. SSO initiatives are often viewed as quick wins relative to user provisioning and role life cycle management projects.

There was one important market acquisition during the latter part of 2009. Microsoft acquired Sentillion and has placed that product's management with Microsoft's Healthcare Solutions Group. Sentillion served only the healthcare industry, and Microsoft has made no announcements regarding plans to sell its ESSO solutions in the broader market. However, we believe this will happen within the next 18 months, creating more competition in nonhealthcare verticals.

The trend to marginally improve product features and effectiveness has continued in 2010 with relatively little resulting product feature differentiation. In 2009, vendors became separated more by their staying power and new customer acquisition. This trend continues in 2010 with the greatest numbers of new customers and seat counts accruing to Passlogix, Imprivata and IBM, and respectable advancement by Evidian, Novell and Sentillion (Microsoft). The remaining vendors have shown only modest gains or have stagnated. The 2009 economic climate played a part in this.

All vendors are being pushed to make their products better support virtualized data center environments and virtualized desktops — particularly those vendors that include a middle tier to their architecture. This requires changes to server software to support virtualization and to endpoint agent software so that it can be accessed through virtual device interfaces. Support for Windows 7 clients has become the norm. None of the rated vendors provide direct support for Mac OS clients. MetaPass is the only vendor we are aware of that claims support for Mac OS and Linux/Unix clients.

There is some momentum for vendors with limited IAM product portfolios to ease into near-neighbor markets such as privileged account activity management (PAAM) and authentication.

Vendors continued the sign-on effectiveness war that never seems to end (and will likely never end). Product enhancement milestones regularly include "improved support for new application types" to ensure that their tools support custom applications and rich interface applications (RIAs) such as those using Java and Flash. As user interface technologies change on client endpoints, this creates new challenges for ESSO tools' sign-on automation because new techniques must be developed to recognize sign-on prompts. Enterprises considering adoption should give special attention to applications with Flash, Java, mainframe terminal interfaces and Unix/Linux terminal interfaces (particularly when older emulators are used), and should require vendors to demonstrate an ESSO product's efficacy with these applications before purchasing.

STRATEGIC PLANNING ASSUMPTION

Microsoft will begin selling Sentillion's ESSO solutions outside of healthcare by year-end 2011, and by 2012 will increase its share of the overall market by 20%.

MARKETSCOPE

This MarketScope was developed using a three-pronged approach:

- We incorporated current information and feedback of Gartner clients via client interactions regarding any issues or problems with the service providers involved in this study.
- We received completed surveys from each vendor. The survey was designed to directly support each of the evaluation criteria used in this analysis.
- We asked for and were provided with client references, which we contacted directly to survey their experiences with the product providers.

Enterprises continue to make tactical investments in ESSO to resolve the problem of users having too many passwords on too many disparate platforms and architectures. Client interest in leveraging Active Directory and using integrated Windows authentication continues as a strong trend in 2010, 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. Increases in Web-enabled applications, coupled with other reduced sign-on technologies, are also proving sufficient for many organizations.

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. These initiatives also limit growth in the ESSO market:

- **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. 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 — for example, a biometric-authentication-enabled application.
- **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 (COTS) 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 bridge tools from vendors such as Quest Software, Centrify, Likewise Software and BeyondTrust. These tools may also have support for integrating custom-developed or COTS Java applications. 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 some integration kits for non-Web applications. Some WAM tools also have limited user provisioning and self-service password reset for applications integrated with the WAM tool. WAM tools can also offer

coarse-grained and fine-grained authorization (also known as entitlement resolution) capabilities. However, some WAM vendors have segmented authorization (also known as entitlement resolution) into separate products. 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. These tools are often not needed when the Web application server environment is homogeneous and the enterprise doesn't need fine-grained authorization, or when a combination of hard-coded application rules and directory groups is used for authorization.

- **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. A trust domain 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. There has also been increased Gartner client interest in OpenID, particularly for consumer and citizen access to enterprise and government services.

Any of these tools can reduce the size of the problem and the number of IDs and passwords to be managed and can potentially mitigate or obviate the need for ESSO.

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 multiple target systems 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, will that be sufficient? If not, then ESSO might be more strongly indicated.

Market Changes: The ESSO market has continued to mature in 2010. With very few exceptions 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 2009 have continued to enhance their customer bases, and have moved more aggressively into geographic markets that were outside their previous territories. However, geographically isolated vendors and even some well-established vendors realized modest customer gains in 2009, and several have seen limited or no net growth.

In late 2009 and through 2010, Passlogix continued to gain significant market share. Its reseller relationship with Oracle has continued to bear fruit, and Passlogix owes a portion of its success to Oracle.

Novell licensed the source code to SecureLogin from ActivIdentity in 2009, and began taking SecureLogin development down an independent path. However, despite having a large legacy installed base of SecureLogin and having a complement of other IAM products, Novell's growth of SecureLogin was more limited in 2009 than we anticipated. 2010 appears to be shaping up as a better year for Novell.

Imprivata again continued to gain customers at an impressive rate in 2009 and early 2010. The company now reports that it is profitable for the first time. Imprivata continues its leveraged use of resellers to grow a predominantly satisfied customer base worldwide.

Gartner estimates that the total 2009 software revenue for the ESSO market was approximately $168 million, and grew at a rate of 8% over the amount reported last year.

Pricing: Pricing dropped for several vendors in 2009 and into 2010, bringing the average prices down by roughly 18%. 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 authentication technologies themselves.
- Three years of product maintenance costs to be included.

The average price for this scenario was $69,000, down from $86,000 in 2008-2009.

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 $219,000, down from $264,000 in 2008-2009.

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 broker between client devices and target systems. Target systems still maintain independent credential stores and will present unique sign-on and password change 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. They may also broker further interaction, such as navigating menus.

Vendor capabilities with ease of target system integration have remained mostly consistent with the 2009 findings; however, the increased prevalence of rich interface applications (RIAs), such as those using Flash, Silverlight or Ajax, have been the new battlefront 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 driven 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.

It is *possible* to get 100% of an enterprise's applications integrated with ESSO tools; however, purchases are cautioned not to sell the idea of 100% efficacy until after proofs of concept (POCs) are conducted. Further, if the organization has dozens or hundreds of applications to integrate that have very disparate interfaces, there is a good chance that some of those applications will not be included in a POC and may be found to be difficult or impossible to integrate. Therefore, it is essential to at least test a representative set of applications; for example, one or more from each class of applications using different user interface technology.

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, post-sign-on automation 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 Versus 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 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 that are difficult or impossible to implement with 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. It is possible to implement a directory instance dedicated to ESSO and separate from the primary enterprise directory. This can help avoid schema extensions to the primary directory; however, attributes needed for ESSO have to be synchronized to the dedicated ESSO directory.

Authentication Technology 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 2010, we have again collected data regarding the use of alternative authentication with ESSO products. There was little change from 2009. 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 provide only 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 "thick client," 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 original equipment manufacturer (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 2010.

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

- **Hitachi ID Systems:** Hitachi ID 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.
- **Ilex:** Ilex provides an integrated platform for WAM and federation (Sign&go) and ESSO (Sign&go ESSO). The same security server is used for all functions and offers global configuration, administration and audit features. A client package is included with Sign&go ESSO. The components are priced separately. The ESSO tool has all the fundamental functions provided by other ESSO products. Ilex, which is based in France, is a relative newcomer to the ESSO field and is currently building its customer base.
- **Softex:** The company had its beginnings as a provider of basic input/output system and device driver software to PC manufacturers, and it has evolved its 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 2010.

Vendors Dropped

None.

Rating for Overall Market/Market Segment

Overall Market Rating: Promising

ESSO remains a requirement for many enterprises. However despite this and its consistent year-over-year growth, fewer vendors are participating in this growth at the expense of others. Even though the word "promising" is used to title Gartner's middle-rating category, this market is past its prime. We believe that new entrants should not expect significant revenues and will face stiff, well-established competition. ESSO is a much smaller market than WAM, user provisioning or the broader authentication markets.

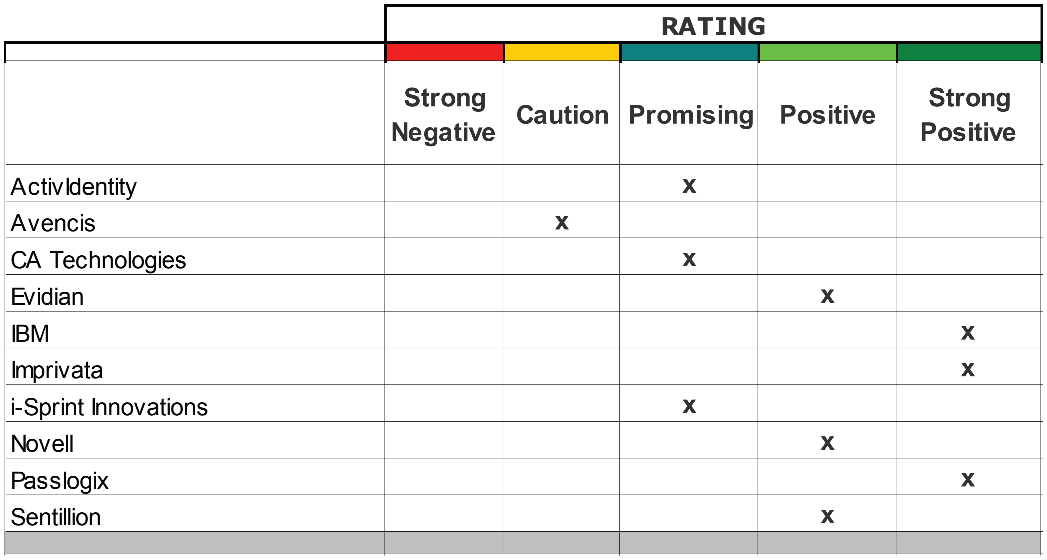
Evaluation Criteria

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 2010)

Figure 1. MarketScope for Enterprise Single Sign-On



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

As of 2 September 2010

Source: Gartner (September 2010)

Vendor Product/Service Analysis

ActivIdentity

ActivIdentity is a long-standing vendor in the ESSO market, having produced or supported acquired products since 1991. Its 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. Terminal-emulator-based applications require the use of a separate "workflow tool" to enable automation. 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 other LDAP accessible directories. ActivIdentity SecureLogin Single Sign-On supports variety of authentication mechanisms, with particular strengths in smart-token integration. ActivIdentity does not have out-of-the-box support for shared workstation fast user switching. However, this can still be obtained through a professional service package.

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. 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. 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. Based on survey data, it appears that ActivIdentity has made progress with increasing seat sales; however, customer growth is unclear, and it is difficult to reconcile this growth with Gartner client interest in ActivIdentity. The majority of ActivIdentity SecureLogin Single Sign-On sales have been to smaller customers. Despite a positive financial turnaround in 2009, we are cautious with regard to its financial statements for the first two quarters of 2010.

Rating: Promising

Avencis

Avencis has excellent breadth of directory support and easy integration, and its SSOX product 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. It improved certificate management with its credential management system that integrates with SSO and provided integration with SAML-based identity providers. The application automation enablement capability was redesigned per customer input and to improve the product's effectiveness.

Pricing for larger implementations is one of the highest among vendors in the market based on the pricing scenarios we described earlier. However, 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.

In 2010, Avencis has gained some new customers with some above-average implementation sizes; however, growth has remained quite flat when compared with market leaders. 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 may be a poor choice for geographies outside Europe. However, despite the overall Caution rating, customers in Europe should still consider Avencis for ESSO.

Rating: Caution

CA Technologies

CA changed its name to CA Technologies this year. 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 Technologies can leverage sales bidirectionally to upsell. CA Technologies has some very large ESSO installations, with one confirmed at 65,000 users. CA Technologies has focused on developing its other more-lucrative IAM toolsets. CA improved the automation wizard to support Java and terminal-emulator-based applications and to support newer operating system and browser levels. We believe that sales for CA Technologies Single Sign-On are static, with most revenue accruing to established customers on maintenance. CA Technologies 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. Its 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.

CA Technologies 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. Customers must pay for a "lite" version of CA Technologies' provisioning product to get SSPR added to Single Sign-On. SSPR is part of CA Technologies' Identity Lifecycle Management offering.

Rating: Promising

Evidian

Evidian maintains a strong presence and sales record in Europe, and has made inroads outside the continent with some gains in the U.S. However, most of its sales and customers are based in France and greater Europe. Customer gains were respectable this year in the face of competition and a tough economy. In addition to the expected ESSO features, 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. This capability can be extended to remote users with an add-on product component. Authentication support is broad and well-integrated with the core product, and plays well to the regional preference for smart card support.

This year, Evidian segmented its authentication support into a separate product called Evidian Authentication Manager. This product can support multiple authentication methods without requiring SSO. It is included with Enterprise SSO, or can be purchased stand-alone. Evidian's product has very good out-of-the-box support for multiple directory products with automated integration for Active Directory. Evidian's product also features a unique shared workstation capability that supports requirements for using multiple workstations simultaneously, for example on trading floors and in laboratories.

Rating: Positive

i-Sprint Innovations

i-Sprint Innovations has made some minor enhancements to its Universal Sign-On (USO) product line and has generated some new business for a small net gain in its customer base. However, growth has been static relative to market leaders and midmarket vendors. USO is part of a larger access management and authentication portfolio that includes WAM and shared account password management. 2009-2010 product enhancements include the addition of a reporting engine for user activity, Java Authentication and Authorization Service (JAAS), and RADIUS authentication support and OTP credential management.

i-Sprint Innovations continues to focus on financial institutions, particularly banks, and in selling its AccessMatrix Universal Sign-On (USO) tools to these firms in the Asia/Pacific region.

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.

Rating: Promising

IBM

IBM successfully accelerated adoption of its Tivoli Access Manager (TAM) ESSO product in 2009 and 2010, and the company obtained new business at a rate on par with other ESSO market leaders. Some very large customers were included in this growth. The company's worldwide distribution, integration and support channels are propelling IBM forward. References reported an overall positive experience with the product and support, but this year, they also

indicated that there were some difficulties integrating some legacy applications and enabling post-sign-on interaction.

IBM began to leverage other parts of its IAM product line for ESSO integration. In 2009, it released Privileged Identity Manager — a combination of Tivoli Identity Manager, TAM ESSO and services that provides shared account password management. 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.

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.

IBM's response to our pricing scenario questions indicates that its retail pricing remains some of the highest in the market. Clients are encouraged to seek lower pricing based on volume discounts.

Rating: Strong Positive

Imprivata

Imprivata has delivered some innovative technical features through development and partnership within the past year. It has integrated video monitoring to support screen locking and logoff when users move away from a workstation, and it has provided the ability to lock the workstation but keep the running application display active to support monitoring activity — both functions could be useful in healthcare and other regulated environments. Their product can now be delivered as a virtual appliance for clients who do not wish to use Imprivata's traditional hardware appliances. The company established technical and business relationships to provide client-side virtual-device interface support for VMware and Oracle Sun Ray environments, thereby enabling roaming user support.

Imprivata has also turned the corner on profitability and continued to heavily leverage its channels to gain a considerable volume of new customers. References and other client feedback indicate that Imprivata's products generally continue to be easy to deploy. There have been a few complaints regarding application integration and endpoint performance, but these have generally been countered by compliments of good support. OneSign has very good authentication integration. OneSign also includes a solid set of canned reports.

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 applications. We have not been able to confirm much uptake of this capability. However, it may be of interest to clients who want to leverage the combination of physical and logical access controls.

Rating: Strong Positive

Novell

In 2009, Novell licensed the source code for SecureLogin from ActivIdentity. Novell also picked up key developer and sales personnel from ActivIdentity in 2009. Installed base remained roughly static in 2009, with signs of healthy growth returning in 2010. Novell has made some improvements to the product in the areas of integration with Novell's IAM suite and some improvements in its automation wizard. Event logging uses industry-standard Syslog format. The automation wizard has been enhanced to support newer application interfaces and operating system levels; however, terminal-emulator support and some custom applications still require use of the scripting interface for automation enablement. Novell's product remains highly capable, and its pricing remains very attractive and one of the lowest in the market.

The iManager plug-in for SecureLogin 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 as a repository, and no Novell infrastructure is required. Novell has a global reseller channel, "follow the sun" support and consulting services to support implementation. SSPR requires the Novell Identity Manager and user application portal.

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

Rating: Positive

Passlogix

Passlogix has continued to show strong growth in customer base and seat count, with some very large deals struck within the past 12 months. Resellers, most notably Oracle, have contributed to this success. Passlogix has demonstrated that its product can scale. It has several very large implementations that serve more than 100,000 users each.

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, yet clients and references still report some of the usual integration difficulties found with all ESSO products. Some target systems can be difficult to integrate and require additional time, and may require code updates from Passlogix.

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. In 2010, Passlogix added the ability to have On Demand load automatically when a Microsoft Forefront UAG session is established. 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 and its new v-GO Universal Authentication Manager (UAM). UAM is a client-only authentication integration shim that supports multiple forms of authentication and can work independently of, or in concert with, v-GO SSO.

Passlogix adjusted its pricing model downward in 2010, and it is much more competitive than in 2009. Passlogix is also bundling shared workstation support, On Demand, and v-GO Authentication Manager (the legacy authentication component for integration authentication methods with v-GO SSO).

Rating: Strong Positive

Sentillion

Microsoft acquired Sentillion in late 2009 and has incorporated Sentillion's offerings into Microsoft's Healthcare Services division. This acquisition gave Sentillion global sales, distribution and support channels for its products. Sentillion had little business outside the U.S. prior to the acquisition.

Sentillion has its roots and strengths in the demanding healthcare industry. In addition to ESSO, the company has provisioning capabilities and strong context management — important for healthcare. Sentillion's products are almost always on our healthcare clients' shortlists for consideration, and Sentillion's SSO tools have demonstrated scalability for large environments. At this time, Microsoft has not made any announcement with regard to selling Sentillion's Vergence or expreSSO products in other industries. We believe that this move will happen within the next 18 months. However, Microsoft is missing opportunities that may begin to "dry up" over time as market-leading competitors extend their leads and when the need for ESSO diminishes in the next two to three years.

Shared workstation support is excellent and provides all required functionality demanded by clinical healthcare environments. References have indicated positive experiences with implementation and ongoing support, with some minor issues being reported around difficulties integrating Java applications. The Java technology wizard was introduced last year in expreSSO but was not part of Vergence. Sentillion indicates that this capability will be included in Vergence by 4Q10.

Rating: Positive

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.