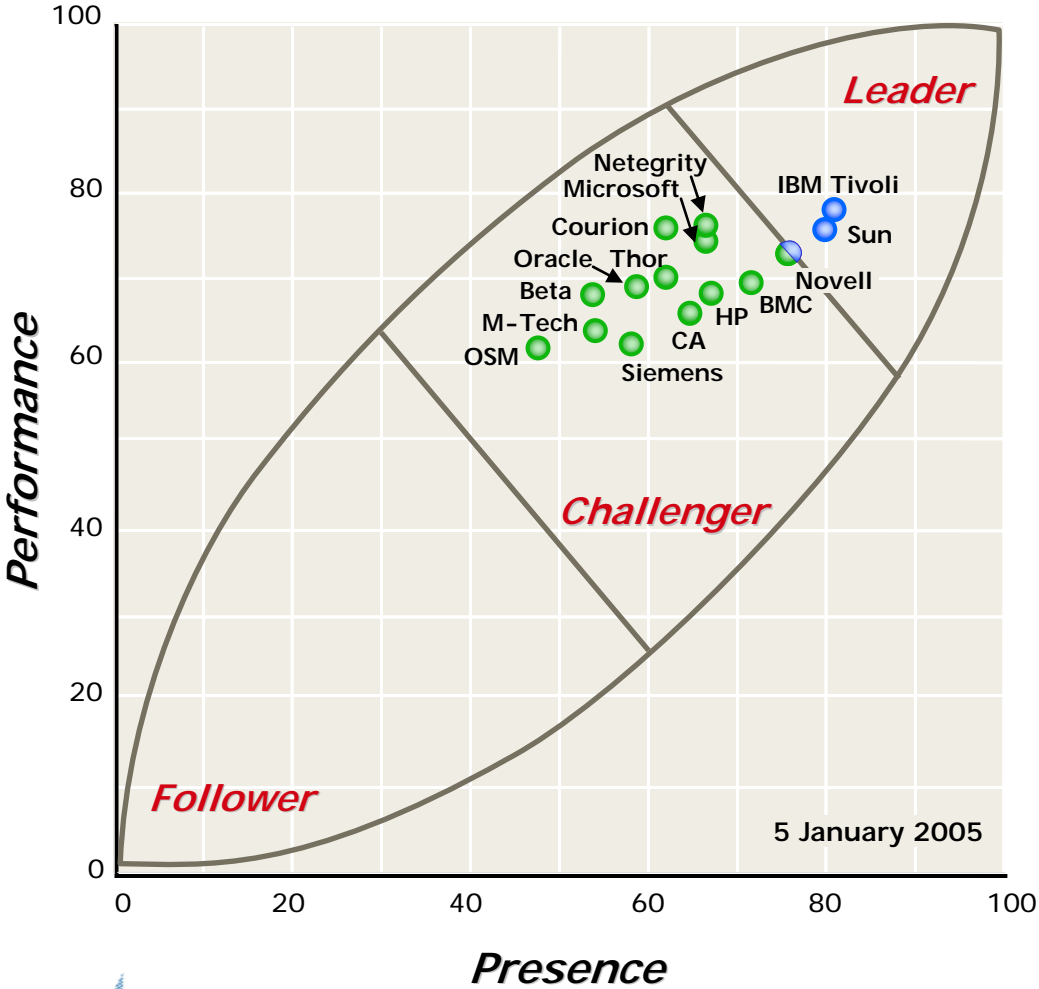




Identity Management — User Provisioning

METAspectrumSM Evaluation



META Group is a trademark, and METAspectrum is a service mark, of META Group, Inc.
Copyright © 2005 META Group, Inc. All rights reserved.

Market Definition

The identity management market predominantly comprises vendors offering technology focused on user provisioning services, enabling enterprises to create, maintain, and retire user identities for network, operating system, and application authentication and authorization access. Solutions may be delivered as part of product suites that also provide workflow services to manage and administer user identities for various identity-related management and delegated administration processes. These include services for password management, logging, auditing, reporting, self-registration, and basic identity repository integration.

Market Forecast

The suite/stack vendors will dominate large-scale opportunities for comprehensive identity management solutions, but component vendors will still have a market opportunity for customers willing to integrate infrastructures and services. Access management, user provisioning, workflow, delegated administration, self-service, password management, and audit/reporting will remain focal points for next two to three years, though requirements for federated identity services management and service-oriented architecture (SOA) offerings will begin to drive new feature needs. Users should expect additional impact requirements for strong authentication, common authorization models, and identity management servicing offerings during 2005-08.

Key Findings

Market standards for identity management involve delivering effective process for identity controls to an enterprise — i.e., user life-cycle management. Key criteria for vendors delivering solutions in this area include their abilities to:

1. Reuse existing infrastructure and systems
2. Integrate provisioning with existing systems
3. Change and modify systems easily over time
4. Scale for volume, security, and performance
5. Adhere to relevant standards (while satisfying the first four criteria)
6. Deploy easily with partners and providers
7. Engender ease of use through their unique combination of features and functions
8. Provide a cost-effective solution

Given that the market is in its early stages, presence and longevity play a vital role — performance, while critical, is secondary. As long as the provider is available, performance can be improved over time. If the provider becomes unavailable, no amount of excellent performance matters. Over time, as the market matures and solutions become better established, this ratio will become more balanced.

To become leaders, vendors must establish a balance among: 1) vision, whereby a comprehensive view of the role identity management plays in their portfolio and how they intend to deliver it is articulated clearly, along with a timeline to achieve it; 2) market share, whereby a critical mass of customers is obtained that demonstrates credibility in the market space; and 3) overall performance, including technology, service, and pricing that is competitive enough to attract and keep customers. The market will become more demanding as the boundaries that define identity management solidify. Users seeking strong identity management contenders should look at vision, partnerships, pricing, market share, technology, and services as key indicators.

Leaders

The most significant characteristics for which leaders demonstrate strength are market presence, major partnerships, services, and some technology leadership, though not necessarily in all cases. In early markets such as this one, technology leaders are not always the winners — quantity sometimes wins over quality. Leaders should be perceived as able to bring multiple resources to bear through numerous channels, providing solutions across many geographies and market sectors.

Challengers

Challengers have distinctively strong technology, in some cases superior to that of market leaders. They just do not have the market presence in terms of geographic reach, market-sector exposure, or partner/channel presence. They provide good solutions and good integration and represent effective choices, but may be ongoing candidates for merger/acquisition, though most of that activity has completed.

Followers

Followers do not view identity management as their core competency, but have products or features that overlap in this space. Although they possess skills and capabilities in identity management and can provide some services, they should not be considered strategic partners in this area and are not likely to enter the market in the near term as major players. They should be considered marginal, tactical solution providers.

Bottom Line

Identity management is a subset of systems management for enterprises, with significant implications to security and risk strategy. At its core, it is not a technology discussion as much as it is a process and organizational discussion about the role of “roles” in enterprises — how people and applications access assets, whether they be applications, databases, or other vital information. The business owns their identity and the assets they are accessing, and the first step to determining how much “identity management” is needed lies at planning levels of the business, security, and IT planning teams.

Business Impact: Without an effective identity management strategy, most enterprises run a substantial risk of being unable to address core compliance, regulatory, audit, privacy, and protection concerns that are topical currently, not only in North America but worldwide. It is not a scare tactic; it is a fact — an effective means of uniformly managing the means of auditing how, when, and what people (employees, business partners, and customers) access is key to mitigating risk and ensuring financial compliance in the enterprise.