

---

## Google Enterprise: Reseller Challenges Arriving

---

In late September 2010, Binary Tree, an enterprise messaging integrator, issued a news release with the blunt headline “Binary Tree Exits Google Enterprise Partner Program.” Although not unknown, playing musical chairs among vendors and their partners is a popular pastime.

What caught my attention was this statement featured in the second paragraph of the news release:

*"It's simply a matter of customer demand," stated Henry Bestritsky, Co-CEO of Binary Tree. "The tremendous uptake we are seeing in the market for migrating to the Microsoft messaging and collaboration platform cannot be ignored. And that includes moving to the cloud-based versions of these solutions like Microsoft's Business Productivity Online Suite (BPOS). The customers we've talked to about moving to the cloud, regardless of their size, have told us that they don't want to move to an e-mail system that offers less functionality and decreases their end user's overall experience."*

There was one other reference in the news release that jarred. The quote was attributed to Stefan af Bjur, the general manager of Binary Tree’s operations in Europe. He makes reference to “specific requirements for privacy and security that haven’t been met by Google’s hosted solutions.”

One unhappy partner is an isolated case. The timing was interesting. Google announced in mid-September 2010 its new two-factor authentication. The idea behind a two-factor authentication method is that you have a mobile telephone, a security device such as a USB key or dongle, and a password. In order to gain unauthorized access to an account, the interloper must have both the hardware component and the password for an account. No security method is flawless, but two-factor authentication thwarts many common attacks.

The two-factor authentication will be available for Google Gmail accounts. The deployment will be staged and completed probably by the end of 2010 or early in 2011. Google has taken an open approach. The Google Authenticator application relies on an open method, RFC 4225. The idea is that developers can build on Google’s two-factor approach.

On September 28, 2010, Information Week reported that Google had embraced OAuth authentication for Google Apps. OAuth is geek speak for “open authentication,” an open standard. Paraphrasing Wikipedia,

With OAuth, users can share photos, videos, contact lists, and other objects stored on one Web site with another Web site. The user nor the site provides the user name and password. The idea is similar to one health club accepting another health club’s member. OAuth uses tokens, not the actual credentials. Each token grants certain rights, often for a specific purpose and a specific period of time. When Tweetdeck interacts with Twitter, access is granted without revealing the user name or password. Google’s support makes clear to me that Google is making progress with its security services.

Google’s enterprise security page provides a run down of the broad security features available to enterprise licensees, developers, and partners. You can access the Google security information at <http://www.google.com/enterprise/security.html>. When I last visited this Google Web page, the company was highlighting its commitment to security, access controls, and what Google calls “secure search in real time.” I am quite interested in search, and Google’s approach seems in line with other vendors of basic enterprise search systems. Google says:

*At crawling, the Google Search Appliance creates an index of information that it has acquired through the various onboard content access mechanisms – the web crawler, file system crawler, relational database crawler, and through the content feed interface. When acquiring and indexing this information, the appliance uses access credentials provided to it by the system administrator. These can include single sign-on (SSO) credentials for forms-based SSO systems, basic-auth credentials, NTLM credentials (username, password, domain), Kerberos, and X.509 client certificates. These credentials are used by the Google Search Appliance to access the content at indexing time.*

A Google savvy programmer can use the purpose-built security methods as well as code specific functions. Google has posted some basic security tips to make certain that users and developers are informed of some security basics. You can access “Keep Your Data Secure” by searching for the phrase at Google.com. For best results, turn off Google Instant. In short, both Google Apps and the Google Search Appliance offer industry-competitive security at this time.

Against these Google security actions, I find the Binary Tree news release and its content out of step. Google continues to add partners, App resellers, and developers. Binary Tree has certainly made an effort to distinguish itself.

In the enterprise market, there are some powerful forces in play. Microsoft may be courting certain companies to abandon their current partner tie ups and ride the Redmond Railroad. If I am correct, I think we will see more partner shifts as integrators and resellers try to strike the

best deal each can. In my experience, the loyalty of an enterprise dance partner is often linked to the revenue a tie up can deliver.

Second, on a higher lever, there is are skirmishes being fought for the cloud. After a slow taxi to the runway, I think cloud enterprise solutions are approaching take off velocity. As a result, organizations are going to be scrutinizing their existing licensing deals and doing some pre-flight checks before moving mission critical applications to hosted service, private clouds, or whatever other buzzword markets slap on remote time-sharing a decade into the 21<sup>st</sup> century. Partners and integrators become much more important because these intermediary organizations often have better relationships with key personnel than a multi-billion dollar Fortune 500 company.

Third, existing enterprise vendors have to circle their wagons. The threat may not be IBM's chasing Oracle customers or Google's efforts to wrest business from Microsoft. The more significant threat may be open source software. In search and content management, open source systems are winning fans and satisfying users in a number of different situations. Cisco Systems, for example, blends open source search and proprietary methods for its newest content-centric systems. Professionals use LinkedIn search to make deals, exchange information, and find work. Some of the plumbing is open source technology with search provided by Lucene/Solr. Consumers get their entertainment fix on Netflix, which uses open source software. Even IBM has embraced Lucene for the search functions in OmniFind 9.x. My view is that partners with a track record are going to be in demand because their expertise provides a first line of defense from community-driven disruption.

In this context, I see the Binary Tree news release as one of the first indicators that partners, resellers, and integrators are becoming more important. To recap, a strong partner can reach people. The Binary Tree news release caught my attention. Second, the fact that Binary Tree makes explicit references to Microsoft strengths and alleged Google weaknesses makes evident the marketing nature of the love affair Binary Tree appears to have with Microsoft. Third, existing partner, reseller, and integrator deals are gaining in importance.

This has several implications. I think the value of certain companies working in these intermediary roles are likely to go up. The client base and billings are important. But perhaps more important are the relationships the best partners, resellers, and integrators bring to a large vendor. Second, the musical chairs game is likely to blur into a "pay to dance" party. Financial incentives and certain sales leads may be more important to an intermediary than the vendor's particular technical approach. Third, partners can provide a buffer between certain vendors and some forces. In addition to open source, there are pressures to reduce on premises direct and indirect costs and delivering more agile systems. A strong partner program insulates or slows down certain types of change within certain client organizations. Often great partners can add friction to a mandated change.

When I think about Google, I see that the company is at a pivotal point in its enterprise initiative. The firm is making progress in security. However, Google must match the other enterprise vendors in three areas: Customer support, ease of use, and perceived value. Google has the resources to become not just a major player in enterprise solutions but the dominant enterprise vendor. Google, however, now faces challenges in a number of markets, not just

STEPHEN E. ARNOLD

the enterprise. Even musical chairs ends and the participants move on. Is the music starting for Google or ending?

Stephen E Arnold, October 1, 2010

Stephen E Arnold is a consultant. His Web site is [www.arnoldit.com](http://www.arnoldit.com). His blog "Beyond Search" is at <http://www.arnoldit.com/wordpress>.