

March 13, 2008

Google Apps Picks Up 2-Factor Authentication

The new two-factor authentication is served up on demand from Arcot Systems and designed to be a lower-cost method to get extra security than tokens or added work from users.

By Lisa Vaas

Google is dead set on convincing businesses that it's safe to move data from under their mattresses to the bank—the bank being Google Apps, of course.

To that end, Google on March 13 introduced two-factor authentication: an extra layer of access security that Google hopes will help to get businesses over the impression that Google Apps isn't enterprise-ready.

Like all of Google Apps—Gmail, Google Talk, Google Calendar, Google Docs, and the recently acquired Postini security and compliance services—the token authentication will be delivered as SAAS (software as a service). The authentication, called Arcot A-OK On-Demand, comes from Arcot Systems, maker of authentication, digital signing and cardholder authentication technologies. It's available to customers using GAPE (Google Apps Premier Edition), for \$1 per user per month, including 24x7 e-mail and phone support.

The new authentication option gives users the same any time, anywhere access to their documents

and data, just with an extra security factor thrown in. That extra layer is transparent to users, who'll have the same user name/password interface, without the need to carry tokens or cards. Available on demand, it requires no software or hardware installation.

The authentication is designed to thwart phishing, keyboard logging, man-in-the-middle, social engineering and other attacks engineered to steal passwords and get at the data stored in Google Apps.

Those types of attacks are of particular concern to on-demand applications, where stolen passwords are a legitimate concern. "A built-in benefit of on-demand software is being able to log in from any Web browser," Gretchen Duhaime, an analyst at Aberdeen, said in a statement. "The potential downside, however, is the threat of login credentials falling into the wrong hands, and sensitive customer information being exposed. Solving this problem is becoming mandatory for anyone who expects to be best in class."

Getting the security concerns off the table is crucial for the SAAS model. After all, SAAS can in fact relieve businesses of a host of labor and expense, said Eran Feigenbaum, senior security manager for Google Enterprise. "One of the beauties for Google Apps is the accessing information any time from anywhere," he said. "On the Internet I can access my data from anywhere I'm at. With that, some companies have some hesitation. [The challenge for Google is to change] that mind-set, from storing your cash under the mattress to storing it in the bank, [changing businesses' mind-set] that that is less secure, and that a user name/password [authentication] is all that's preventing people from accessing my information."

Carol Alexander, vice president of marketing for Arcot, agreed, saying that the appeal of the security SAAS approach is that it's a relatively inexpensive way to get strong authentication without the need to buy tokens and with no effect on users.

Reprinted from eWEEK, March 13, 2008 with permission from Ziff Davis Enterprise Inc.
©2008 Ziff Davis Enterprise Holdings Inc. All rights reserved.