NETWORKWORLD

# Single sign-on moves to the cloud

Okta and OneLogin score high in test of eight SSO solutions that cut help desk calls and boost password security

*By David Strom, Network World*

*December 17, 2012 12:00 AM ET*

Network World - We are awash in passwords, and as the number of Web services increases, things are only going to get worse. Trying to manage all these individual passwords is a major problem for enterprise security. Many end users cope by re-using their passwords, which exposes all sorts of security holes.

One solution is a single sign-on (SSO) tool to automate the logins of enterprise applications and also beef up password complexity, without taxing end users to try to remember dozens of different logins.

SSO isn't new: we have had various products for more than a decade. What is new is that several products now combine both cloud-based SaaS logins with local desktop Windows logins, and add improved two-factor authentication and smoother federated identity integration.

Also helping is a wider adoption of the open standard Security Assertion Markup Language (SAML), which allows for automated sign-ons via exchanging XML information between websites.

**Cloud-based single sign-on:** A business perk for customers?

The SSO market includes more than a dozen products from boutique shops to large software vendors. We tested eight products: SecureAuth, OneLogin, Okta, Symplified, Intel's McAfee Cloud Identity Manager, Numina Application Framework, SmartSignin and Radiant Logic. Several other SSO vendors were contacted but decided not to participate, including IBM, CA, Oracle and Ping Identity. (Watch a slideshow version of this story.)

## SmartSignin

Like McAfee, SmartSignin has two separate offerings: one cloud-based and one for on-premises. The latter is only available at the higher Enterprise price. The product is still in beta and features are being added rapidly. They integrate with three identity providers at the moment: Google Apps, AD, and Salesforce.com. The company is small but seems to be on the right track.

For example, SmartSignin seems to be paying a lot of attention to various security exploits, which is a good thing. It is the only one of the SSO products we tested that not only requires a password but a separate passphrase that you and you alone have knowledge of, and that you have to enter when you sign-on to their SSO portal. All security information is stored on your desktop. Their Active Directory connector doesn't transmit information in the clear in order to protect against man-in-the-middle attacks of your directory content.

They are weak in terms of browser support and are just getting started on their multifactor integration. The Enterprise package has a single option for out of band authentication using text SMS messages. They claim more than 400 applications are supported and pre-configured.

Their dashboard is well-designed and easy to navigate. There is a single report that is just a listing of events, which is less than satisfying.

Pricing for the Enterprise plan for 500 users would be $43,200 for the first and subsequent years. If you can do without the Enterprise features (multiple roles and on-premises server), then the Pro plan will bring this down to less than half that amount.