There are numerous choices available for adding stronger authentication into a current username and password authentication model, says Michael Lipinski.

By now we all know what multifactor authentication is and does. So the question becomes, why shouldn't everyone be using it. Simply stated, as a business, we want to know that it is really you accessing your private information. As a user of a service, I want to know that no one else can pretend to be me and gain access to my information. It is no longer prudent for an organization or an individual protecting sensitive information to rely solely on a simple username and password as their only form of protection.

There are numerous choices available for adding stronger authentication into a current username and password authentication model. Whether accessing a PC through Active Directory/Lightweight Directory Access Protocol credentials, accessing secure web applications or doing banking online, there are numerous options that should fit any budget or need.

# Entrust IdentityGuard v9.3


| | |
|---|---|
| **Vendor** | Entrust |
| **Price** | $8 per user for one,<br>$3 per user for 25,000 |
| **Contact** | www.entrust.com |

Entrust IdentityGuard is an open, versatile authentication platform that enables security across diverse users, transactions and applications. This authentication platform provides a range of authentication capabilities, allowing organizations to match the appropriate authentication method to user experience, security requirements and cost, rather than relying on one single authenticator.

SC MAGAZINE BEST BUY

The tool is typically deployed on Microsoft Windows Server 2008 R2 using the integrated application server, or in Oracle WebLogic Server 10g R3 and IBM WebSphere Server 6.1 application server environments. Entrust IdentityGuard 9.3 also can be deployed on Windows Server 2008, 2003, 2003 R2, IBM AIX 5.3, Sun Solaris 10, and Red Hat Enterprise Linux 5.x. It is also supported on many virtualized environments.

The product was provided for us as a virtual machine. We did run through the application load to see what was involved. It did take some work, but it was nicely automated. We ended up testing with the fully configured VM since it had the sample applications with which we could test the multitude of authenticator options. The administration interface is web-based or accessed through the program tab on the server itself. We found the interface clean and very easy to use.

Entrust has a wide array of supported authentication types, including any OATH-compliant tokens, machine-based, knowledge-based, one-time password (OTP), grid, eGrid, token, x509 certificates and geolocation. New to this 9.3 release is support for mobile device soft tokens. We were provided with and tested an iPod with an Entrust application that turned the device into an OTP solution.

Tokens come with one year of support. Support for the software is available for a fee with options ranging from eight-hours-a-day/five-days-a-week to 24/7. There are too many support options to fully discuss here. This is a full-featured offering for identity and authentication.

**SC MAGAZINE RATING**

| | |
|---|---|
| Features | ★★★★★ |
| Ease of use | ★★★★☆ |
| Performance | ★★★★★ |
| Documentation | ★★★★★ |
| Support | ★★★★★ |
| Value for money | ★★★★★ |
| **OVERALL RATING** | ★★★★★ |

**Strengths** Full offering, well priced.
**Weaknesses** Did not find any.
**Verdict** With all the options supported, this solution delivers true, layered multifactor identity and authentication management. We give this our Best Buy.





This solution delivers multifactor identity and authentication management. We give this our Best Buy.

Michael Lipinski