

When it comes to email security in the enterprise, removing user interaction helps to ensure that corporate policy is truly enforced, says **Nathan Ouellette**.

Similar to other information security threats, securing enterprise email has been a growing concern for many organizations. There are several important reasons to investigate technologies that help an organization control the use of email within the corporate environment. Confidentiality

of email messages is one of the most important issues facing enterprises that deal with personally identifiable information. Ensuring that sensitive information is properly protected and preventing data leakage are not only abest practice concerns, but also compliance issues across many regulations.

Another concern is message integrity. Client-side email attacks, phishing, and spam have information security managers taking notice. Sophisticated methods for infiltrating organizations have turned to email-based attacks using a combination of techniques to trick users into opening back door channels.

Entrust v9.1



Vendor Entrust

Price: \$5000

Contact www.entrust.com

The Entelligence Messaging Server v9.1 is an appliance-based email gateway that provides encryption and digital signing of messages internally and externally to the organization. The Messaging Server is part of Entrust's Entelligence line of encryption products. The product uses open standards, such as S/MIME, OpenPGP, and it also includes support for DKIM. Although encryption and signing are the primary uses of this appliance, third-party content scanners can integrate into its centralized policy mechanism.

The product is flexible and easy to use out of the box and, from an enterprise perspective, it includes a multitude of encryption options. As one would expect from a more holistic solution, the product integrates email security with as much transparency to the user as possible. After initial setup and stepping through the wizard-driven interfaces, we were able to integrate the solution into our test environment with ease.

Performance-wise we were impressed with Entrust's product. All the bells and whistles for an email security defense are present within the solution. Automated and seamless email security, as well as user-controlled encryption, are options based on the policy of the organization. Webmail push-and-pull delivery for external recipients, secure PDF delivery and support for DKIM make this a strong solution with many features. One option that impressed us was support for mobile clients. Although true content filtering is not built into the solution, the tool can scan messages for keywords in order to determine if sensitive information is present and how it should be treated.

Entrust offers three levels of support, as well as additional consulting services as needed. Support is offered via telephone and email. In addition, the Entrust support site contains white papers, documentation and a customer support portal.

The \$5,000 price does not include the cost of user licenses. User licenses are \$50 per user for a perpetual license and \$25 per user for a subscription license. The cost of the solution is a great value and puts this tool at the top of the heap with regard to enterprise email security solutions.

SC MAGAZINE RATING

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Great set of email security features; support for DKIM.
Weaknesses None that we found.
Verdict Fantastic value given the price point and feature set. A truly competitive player in the email security space. This is our Recommended product.



Great set of email security features; support for DKIM.

Nathan Ouellette

Entrust[®]
 Securing Digital Identities
 & Information

Entrust
 Worldwide Headquarters
 One Hanover Park, 16633 Dallas Parkway
 Suite 800, Addison, Texas, USA 75001
 North America Sales: 1-888-690-2424
 EMEA Sales: +44 (0) 118 953 3000
 Email: entrust@entrust.com