

Organizations are dealing with sophisticated spam attacks, phishing, botnets, mandates and other risk areas that must be managed, says **Nathan Ouellette**.

As the reliance on messaging continues to grow and the value of information increases exponentially, organizations are looking to protect messaging services from vulnerabilities and evolving threats. Inbound and outbound email services represent a tremendous risk to any enterprise,

whether the threats are malicious outside attackers or simply human error from a corporate perspective. Organizations are dealing with sophisticated spam attacks, phishing, botnets, regulatory compliance mandates and several other risk areas that must be managed in order to effectively secure information.

Email content management vendors have recognized the need for more granular control over email security. Features and options continue to converge as appliance vendors are responding to the need to secure malicious inbound emails and data leakage concerns for outbound messages.

Spam and Virus Blocker



Vendor Cisco
Price starts at \$2,599
Contact www.cisco.com

Cisco's Spam and Virus Blocker is a single hardware appliance that is marketed to small businesses and can support up to 250 users. The device acts as an email gateway and message transfer agent, typically deployed between the internet edge and the email server. The appliance secures email using anti-malware, anti-spam as well as content filtering.

Configuration of the product is done remotely via a web interface. The setup was fairly easy and straightforward. The quick-start guide provided with the appliance was useful and we were able to connect to the administrative interface and implement key features in a short amount of time.

Changing views and navigating content is not done from the left side as we often see in many

web interfaces. When it came to viewing information on the system dashboard, we had to navigate back to the dropdowns provided at the top of the page and choose a different view since the dashboard views are not customizable. Given this small nuance on the dashboard, the device itself has all the features we would expect. Reputation-based validation, anti-malware, LDAP integration, content filtering using dictionaries, as well as smart identifiers (Social Security, credit card numbers, etc.) were all part of the solution.

It took us a few minutes to realize that the dictionary files need to be loaded one by one from a separate directory on the appliance. Once they are loaded, there are hundreds of industry and compliance related keywords that the device can use for content filtering. The administrative features on the device are impressive and contain features you would find on larger scale enterprise-class solutions.

The online help file seemed a bit light on the content. However, it should provide adequate direction for administrators.

No-cost 24/7 phone and email support is included. This includes a warranty on the hardware and updates to the software. The support website is top notch.

This is an impressive device as an entry point into the small business market. Smaller organizations with the budget and need for granular security options will appreciate the full featured enterprise-class nature of the product, as well as the support.

SC MAGAZINE RATING	
Features	★★★★★
Performance	★★★★★
Ease of use	★★★★★
Documentation	★★★★☆
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★
Strengths Great set of features and administrative capabilities for small businesses.	
Weaknesses Dashboard is not customizable, documentation is a bit light.	
Verdict An impressive value with regards to features and price point.	



Great set of features and administrative capabilities for small businesses.

Nathan Ouellette



www.cisco.com/go/blocker