

Rogue access points can blow your organization's security apart, but there are products out there that will not only find them out, but also offer integrated wireless management, says **Peter Stephenson**

Wireless networking has become almost analogous with insecurity. Although there are many techniques to lock down WLANs, many are forgotten or misconfigured. Assuming an insecure environment, *SC Magazine* looked at several products which

can detect vulnerabilities on a wireless network and aid in quick remediation. Whether the risk was from accidental configuration errors, rogue access points or active attackers, we were looking for tools which could help administrators quickly address the potential

threat. We received a variety of products including packet analyzers and wireless sensors, with approaches varying from passive packet analysis to aggressive network filtering. Put together, these tools can ease the challenge of securing your wireless networks.



## BlueSecure



**Supplier** Bluesocket  
**Price** Sensor \$695; software \$2,250  
**Contact** [www.bluesocket.com](http://www.bluesocket.com)

BlueSecure from Bluesocket is a leader in its field. Why? Because while most wireless security products are not able to detect anyone walking up with a wireless capable computer and connecting to their network, BlueSecure detects computers, access points, or any other type of wireless connection device.

BlueSecure creates a system that will detect all wireless devices including a/b/g RF ranges within the sensors range. It also can create reports and send them via email to the administrator, so that they do not have to constantly

monitor the system. BlueSecure also supports the capability to shut down rogue access points that it is either unsure of or known to be rogue points.

The device offers its clients full system integration – it can track and maintain the status of all access points and wireless connections within sensor range. With this capability it puts BlueSecure ahead of the competition.

It has the capabilities of normal tracking and reporting software for networks. It can detect certain types of hacker attacks, such as war driving attacks. This ability to detect and stop attacks through the air waves leaves the users of BlueSecure a step ahead of the competition, because most do not detect intrusions until after the system has been compromised.

Every vendor must provide technical support to their clients to complete the sale. Bluesocket provided high-quality support to all needs addressed during the installation and setup of the software. It gave me a personal representative to help me with any and all questions and setup problems, who was still available for questions on any operations of

the software and hardware even after initial setup.

Many companies send you through an ACD network before giving you to a technician who most likely read answers to problems from a book that has been built with most problems. But Bluesocket technicians are well versed in the workings of their software in both setup and troubleshooting of problems.

In all, this software is well worth the cost of nearly \$3,000 for both the software and hardware to protect your network.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★☆
Performance	★★★★☆
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
<b>OVERALL RATING</b>	<b>★★★★★</b>
<b>For</b> Pricing, full system integration, ability to detect attacks early.	
<b>Against</b> Might be a bit tricky to set up and integrate with other enterprise security programs.	
<b>Verdict</b> Powerful early-warning system with the ability to lock down threats the moment they appear.	

Powerful early-warning system with the ability to lock down threats the moment they appear.

**Peter Stephenson**

For more information about Bluesocket WLAN solutions, please contact us today at:



Bluesocket, Inc.  
 10 North Avenue  
 Burlington, MA 01803  
 USA  
 866-633-3358

Or visit our Website, [www.bluesocket.com](http://www.bluesocket.com), for a Bluesocket office nearest you.