



PRODUCT EVALUATION GUIDE

Wireless Security Vendors

Insight's Technology Assessment Services (TAS) team has evaluated wireless security products from the following vendors:

- Bluefire
- Bluesocket
- CREDANT Technologies
- Good Technology
- NetMotion Wireless
- Symantec
- Trend Micro
- Trust Digital
- Vernier Networks

SECURING THE WIRELESS ENTERPRISE

After a rocky start, wireless LAN technology is beginning to gain acceptance in the workplace. Initially, enterprises were slow to adopt wireless initiatives because of security concerns resulting from the failure of Wired Equivalency Protocol (WEP) to provide adequate protection.

In an effort to overcome this hesitancy, many vendors now offer products that can secure your wireless network by providing an end-to-end virtual private network (VPN) from the remote laptop to the network. These switches can sit at the edge of your network or in centrally located wiring closets, providing a VPN termination point for remote users.

The new wireless security solutions address WEP's weaknesses directly, providing secure authentication, authorization and encryption. They offer an easy way to centrally manage a large number of access points, simplifying your WLAN by terminating multiple access points so you can control bandwidth usage and monitor the performance of your network. Roaming and session persistence allow users to move around freely from network to network while maintaining session connectivity.

KEY CONSIDERATIONS

Infrastructure

Development of a sound security policy is the most important first step. Rogue access points probably already exist—if you don't have a company policy and enforcement plan, you will lose control over your network.

When you are choosing a wireless security solution, here are some other important points to keep in mind:

- **Access point selection** - Choose enterprise-class 802.11 access points (APs) that support your standards and protocols.
 - If you're using the 802.1x authentication protocol, make sure the AP supports it.
 - Power over Ethernet (POE) support eliminates the need to have power installed at each AP location, and could mean significant cost savings. Know whether or not your AP choice supports POE.
 - APs with high-grade antennas that produce strong, tight signals will help prevent leakage outside your desired coverage area.
- **Database compatibility** - Search for a solution that can use your existing authentication database (i.e. RADIUS, LDAP, etc.), so you don't have to create and maintain a separate database.
- **User policies** - Determine who really needs wireless access and what they need access to. Treat your WLAN as an unsecured network, the same way you would your remote access network.
- **Data encryption** - If users need LAN access from suspicious external "hot spots" such as a coffee shop or an airport, use a VPN solution to encrypt data from end to end.



- **Authentication** - If you're using the 802.1x authentication framework, determine what authentication method works best for your situation. If you have an existing PKI infrastructure, EAP-TLS may be your best and most secure choice. Otherwise, consider PEAP or EAP-TTLS, which is still very secure.
- **Scalability** - Make sure your solution can scale up to a larger network, should you need it to.

KEY PRODUCT FEATURES

To make sure you understand the functionality you need, be sure to conduct a thorough analysis of your infrastructure. Unnecessary features may produce unwanted licensing costs or network overhead, while a solution lacking critical features may result in failure to mitigate your organization's specific risks.

- **Centralized management of access points** - Remotely manage and apply policies to distributed access points.
- **Roaming and session persistence** - Move a wireless client from one network to the next without interrupting session connectivity.
- **COS (Class of Service)** - Throttle wireless client bandwidth usage, to keep one person from using all the available bandwidth.
- **Gateway fail-over support** - Guarantee your wireless network can provide 100% uptime by switching over to a standby unit when necessary.
- **802.1x support** - Ensure secure, mutual authentication between the client and an access point.
- **Virtual Private Networking** - Provide end-to-end secure and encrypted sessions over unsecured networks.
- **Load balancing** - Distribute session loads across several servers, keeping session performance at its peak.
- **Fail-over** - Make sure sessions roll over to another server, in the event of a server failure.
- **Server pooling** - Manage several wireless controllers as one logical server.

CONCLUSION

Wireless access switches provide the security necessary for a wireless LAN deployment, and address wireless security failures of the past. These products prove that, with a strong wireless security policy, careful selection and placement of your access points, and the right wireless security solution, implementing an 802.11 network can be a successful initiative that will allow your IT department to sleep well at night.

Insight has sales specialists ready to discuss your wireless security needs, and a supporting staff of technical resources. We can be a valuable resource when you're faced with the diverse issues that may arise in your effort to secure your organization's wireless network.

For more information, contact your account representative, or the Insight Technology Assessment Services team at tas@insight.com

Insight and the Insight logo are registered trademarks of Insight Direct USA, Inc. All other trademarks, registered trademarks, photos, logos and illustrations are the property of their respective owners. ©2007, Insight® Direct USA, Inc. All rights reserved.