

UNSTRUNG INSIDER

UNSTRUNG'S TECHNOLOGY RESEARCH SERVICE FOR FINANCIAL PROFESSIONALS, INVESTORS, AND LEADERS IN THE WIRELESS COMMUNICATIONS/NETWORKING INDUSTRY.

Intrusion Detection and Prevention for 802.11 Wireless LANs

TABLE OF CONTENTS

- I. Introduction: Look Who's Lurking
 - **Wireless IDS: A Vital Component of Large Enterprise Wireless LANs**
- II. What a Wireless IDS Does, and Why
 - **How They Work (Introductory Guide)**
 - **Why You Need Detection and Prevention**
 - **Categories of Wireless IDS Vendors**
 - **Wireless IDS Capabilities**
 - **Wireless LAN Attacks**
- III. Product Comparison
 - **Handheld Monitoring**
 - **Monitoring Sensors**
 - **Access Point Monitors**
 - **Appliances, Switches, and Servers**
 - **Managed Services**
- IV. Vendor Product Analysis
 - **Profiles of 11 Wireless IDS Products**
- V. Startup Financial Analysis
 - **Funding Details**
 - **Headcount Data**
- VI. Conclusion

January Highlights

- **Wireless IDS will soon** become vital to large enterprise wireless LANs – major infrastructure vendors know this and are set to incorporate this feature into their portfolios.
- **OEM deals between IDS** startups and equipment providers are imminent – product lab testing has already begun
- **Cisco, Nortel, Extreme, Symbol, and others** need IDS features to match the startups' capabilities and will move soon to plug the gap
- **Aruba's wireless IDS** features are the most advanced of any network infrastructure vendors'
- **AirDefense appears to be** the leader in terms of market perception and customer wins, but it must develop an OEM licensing model soon
- **Network Chemistry's** and AirMagnet's embrace of OEM licensing and low-cost products is the most viable startup strategy
- **IDS analysis agents will** ultimately be distributed across laptops, PDAs, APs, and dedicated sensors