WIDS Checklist: Is Your Business Ready?

A Technical Evaluation for IT Managers & CISOs

As enterprise networks grow, the gap between managed and visible widens. This checklist helps you identify where your wireless security perimeter ends and where your risk begins. Use this to evaluate your current infrastructure and determine if a Wireless Intrusion Detection System (WIDS) is your next logical step.

☐ **Inventory Accuracy:** Can you currently identify every wireless device in your building, including those not connected to your network?

☐ **Rogue Detection Speed:** If an employee plugs in a $20 home router today, how long would it take your team to find it? (WIDS is required if answer is >24 hours).

☐ **Neighboring Networks:** Do you have a list of authorized neighboring Wi-Fi signals? Can you distinguish them from an attacker's Evil Twin signal?

☐ **IoT Discovery:** Can you identify headless IoT devices (printers, smart sensors, HVAC) by their radio frequency fingerprint rather than just their MAC address?

☐ **Audit Logs:** Can you provide an auditor with a 6-month historical log of all detected wireless threats?

☐ **Requirement 11.1 (PCI-DSS):** Are you currently performing manual quarterly scans for rogue APs? (WIDS automates this).

☐ **Data Privacy (HIPAA/GDPR):** Is your guest Wi-Fi physically and logically separated from your internal network, and is it monitored for Man-in-the-Middle sniffing?

☐ **Proof of Mitigation:** If an attack occurs today, do you have a system that records the exact duration and nature of the breach for insurance and reporting purposes?

☐ **Deauthentication Alerts:** Does your current system alert you if a deauth attack is forcing your executives' laptops off the network?

☐ **Spoofing Detection:** Can your network detect if an unauthorized device is broadcasting the exact same SSID (Network Name) as your corporate Wi-Fi?

☐ **Signal Triangulation:** If a malicious device is detected, can your IT team locate its physical position (X, Y coordinates) within your building using your management console?

☐ **RF Jamming:** Can you distinguish between bad Wi-Fi signal and Denial of Service (DoS) jamming attack?

☐ **AP Count:** Does your environment have more than 50 Access Points?

☐ **Multi-Site Management:** Do you manage remote branches or retail locations without on-site IT staff to perform manual security sweeps?

□ **IT Overhead:** Is your team spending more than 5 hours a week troubleshooting mysterious wireless connectivity issues?

Scoring Your Readiness

- **0 - 4 Ticks:** Your current wireless security is likely *sufficient* for a small office environment.
- **5 - 9 Ticks:** You have significant blind spots. You are at *moderate risk* for a rogue AP or IoT-based breach.
- **10+ Ticks:** *WIDS Deployment Recommended.* Your network scale and risk profile have outgrown standard security. You require 24/7 automated airspace monitoring to remain secure and compliant.

Don't wait for a failed audit or a data leak to secure your airspace.

Browse our marketplace for Network Security Solutions. *Compare leading providers like Cisco and Aruba to find the right fit for your enterprise architecture.*