



# Wireless Assessment & Security Test

## DATASHEET



## Put Your Wireless Network to the Test

Wireless networks are everywhere—and while the power productivity, they also introduce security risks. Simply using password protection is no longer enough. Wireless Intrusion Prevention and Detection Systems help, but even then, you can't be certain your environment is secure. With attack methods becoming more advanced every day, it's essential to conduct physical testing of your wireless infrastructure to understand what a potential attacker could access.

You likely have an internal wireless network for employees, a guest wireless network for visitors—or both. These networks are visible to anyone in range, even if they aren't open to public access. This visibility makes them a potential entry point for cyber attackers. OneMind's Wireless Assessment & Security Test (WAST) helps you uncover and secure those vulnerabilities before someone else does.

## Testing Methodology

Our Wireless Assessment & Security Test (WAST) provides a thorough evaluation of your wireless environment through simulated attacks and vulnerability analysis.

**Our process includes:**

1. External wireless scanning to identify network attack vectors
2. Manual vulnerability testing
3. Review of wireless device configurations
4. Assessment of wireless policies
5. Wireless topology mapping

If conducted onsite, our analysts will also walk through your physical location to test the signal range and ensure your wireless network isn't unintentionally overextended.

You'll receive immediate alerts for any critical risks discovered, followed by a full, detailed report including actionable recommendations to help secure your wireless environment.

---

## A Wireless Assessment & Security Test Includes:

- ✓ Manual vulnerability testing
- ✓ Wireless device configuration review
- ✓ Wireless policy review
- ✓ Wireless topology mapping

## Frequently Asked Questions

**If I only have an internal wireless network with no public access, do I still need to have it tested?**

Yes. Even private/internal networks are susceptible to threats—especially from nearby actors who can see the network.

**How often should we perform this type of testing?**

Typically, once or twice a year is recommended. However, testing should also be conducted after any significant changes or upgrades to your wireless environment.

**What if I have multiple wireless networks? Can you test them all in one assessment?**

Absolutely. We can include multiple networks in a single engagement. Pricing is based on the number of wireless networks included in the scope.