

WIRELESS PENETRATION TESTING

Attacker techniques applied to your wireless infrastructure and devices.

Wireless networks expand your connectivity, and your attack surface. We simulate attacker techniques to uncover weaknesses in your wireless environment, from rogue access points to weak encryption, across the infrastructure, devices and protocols behind it.

TEST YOUR AIRSPACE THE WAY AN ATTACKER WOULD.



WHY DIGITALERA

Attacker emulation

Testing emulates actual attacker behavior in your environment.

On-site expertise

In-person assessments handled with discretion and precision.

In-depth reporting

Technical findings through executive insights, built for action.

Compliance-mapped

Results map to frameworks as evidence for audit readiness.

WHAT YOU CAN EXPECT

- Insight into real-world wireless vulnerabilities
- Misconfigurations and insecure access points found
- Encryption, authentication and segmentation recommendations
- Clarity on user device risk and network visibility
- Support for PCI DSS, ISO 27001 and NIST wireless controls

WHAT YOU RECEIVE

- ✓ Wireless vulnerability report
- ✓ Findings with impact analysis
- ✓ Prioritized recommendations
- ✓ Executive summary and debrief

How it's scoped

Project-based, scoped on a discovery call. Testing includes on-site work, so access is planned with your team.

Right fit if you run Wi-Fi across offices, guest or branch networks, or need wireless evidence for PCI DSS or ISO 27001.

Something else first if you want coverage and performance mapped (Network Assessment) or your concern is the wired internal network (Internal Penetration Testing).



Talk to an expert

digitaleragroup.com/contact/penetration-testing

Active incident? Certified responders answer 24/7, no retainer required.

CALL US: 1-786-621-8600