

WIRELESS NETWORK ASSESSMENT SERVICES

Keep Users Connected and Attackers Out

Wireless networks keep users connected, but misconfigurations, rogue devices, and poor security coverage can leave internal assets exposed.

Organizations need a clear, actionable picture of their wireless security posture before attackers find the gaps. With a Wireless Network Assessment, GuidePoint Security's certified offensive security experts identify rogue devices, coverage weaknesses, and misconfigurations that expose internal environments to unauthorized access. GuidePoint delivers prioritized recommendations to reduce the wireless attack surface, close coverage gaps, and strengthen the overall security program.

Strengthening Wireless Security Through Continuous Assessment

Attackers can probe wireless networks at any time, from anywhere within signal range, even from a parking lot or neighboring building. Meanwhile, these environments continuously evolve through infrastructure changes, device proliferation, environmental shifts, and emerging threats. Security teams are trying to safeguard their wireless networks while also under intense scrutiny from auditors, regulators and insurance carriers.

GuidePoint Security helps organizations get ahead of evolving threats, reduce wireless network risk, and maintain compliance. Our Wireless Network Assessment services provides an ongoing cadence of proactive wireless security evaluations.

Continuous, proactive assessment helps organizations catch and fix issues such as:

- ✓ **Closing unintended access opportunities** caused by signal footprint exposure extending beyond physical boundaries
- ✓ **Strengthening authentication and encryption** before attackers intercept traffic or gain network access
- ✓ **Sealing configuration gaps** before they silently expose internal usernames and domain information to passive observers
- ✓ **Shutting down rogue access points** and unauthorized devices operating within or adjacent to the environment
- ✓ **Fixing segmentation failures** that might allow wireless clients to reach sensitive internal assets
- ✓ **Finding detection and response gaps** that leave suspicious wireless activity unnoticed
- ✓ **Maintaining compliance** across applicable regulatory requirements and security frameworks



Stronger Together. Protecting What's Next.

Working with GuidePoint, your organization will be backed by our elite team of highly-trained cybersecurity engineers, architects and consultants who come from organizations of all sizes, including Fortune 100 companies, the Department of War, and U.S. intelligence agencies.



The Wireless Network is Only as Secure as its Weakest Signal

GuidePoint Wireless Network Assessments give organizations objective evidence of where wireless controls are working and where they are not. Our certified offensive security experts begin with a contextual understanding of each customer's environment coupled with a thorough understanding of how threat actors operate against wireless infrastructure. We rigorously evaluate the environment for weaknesses and provide recommendations based on potential real-world impact. This approach transforms complex wireless security findings into an actionable plan for prioritized remediation.

The result is a clear path toward a hardened wireless environment, validated security controls, quantified risk exposure, and the stakeholder confidence that comes from knowing wireless infrastructure can withstand real-world attacks.

Uncover Hidden Weaknesses in Wireless Infrastructure

GuidePoint evaluates wireless environments using a comprehensive assessment framework that systematically examines the wireless attack surface. We find the issues that threat actors exploit to gain unauthorized access to internal networks, including:

- Initial configurations or significant changes to the physical environment, coverage areas, or access points that could introduce security gaps
- Network segmentation or policy changes that might weaken wireless client isolation or access controls
- Wireless-related security incidents that have exposed gaps in visibility, monitoring, or defensive controls
- Rogue devices, unauthorized access, or suspicious wireless activity threatening critical assets
- Expanding device populations, including Bring Your Own Device (BYOD) and Internet of Things (IoT) systems that carry with them new wireless attack surfaces
- Evolving business operations, office expansions, or infrastructure growth that create new areas of wireless risk

GuidePoint validates every finding to eliminate false positives and ensure remediation efforts are focused where they matter most. We align prioritization with trusted frameworks including NIST and industry best practices, helping organizations strengthen wireless security posture while supporting compliance objectives and operational resilience as environments grow and evolve.

Why GuidePoint Security

When cyber threats target your wireless environment, you want the best on your side. GuidePoint Security designs, deploys, and delivers tailored cybersecurity solutions that drive real results. We validate security across any environment, faster, smarter, and with less risk to strengthen your defenses. Accelerate your business with confidence and protect what matters most.

About Us

GuidePoint Security brings together proven expertise, great relationships, and leading technologies to solve our client's most complex cybersecurity challenges. As a trusted cybersecurity advisor and partner, GuidePoint keeps people, data, and operations safe. We deliver tailored cybersecurity services that adapt to safeguard the nation's leading organizations today and provide complete confidence in their cybersecurity tomorrow. Stronger Together. Protecting What's Next.