WatchGuard®

Trusted Wireless Environment

Don't let Wi-Fi be your biggest security gap. Hackers prefer to go after the weak link in the security chain and it doesn't take much to hack into the Wi-Fi network using easily accessible tools and a plethora of online how-to videos. What's worse – your business networks become compromised due to malware implanted and credentials stolen over Wi-Fi, and it can cost millions in fines and breach remediation expenses to fix.

You need a **Trusted Wireless Environment**, a framework for building a complete Wi-Fi network that is fast, easy to manage, and most importantly, secure. Your employees, vendors, and guests rely on you to keep them safe and it is your responsibility to be knowledgeable about Wi-Fi security risks and how they impact your organization. You need a solution that delivers on the following three core pillars:

1 MARKET-LEADING PERFORMANCE

You should never be forced to compromise security to achieve adequate performance to support your environment with the speed, connections and device density that it needs.

2 SCALABLE MANAGEMENT

With easy set-up and management, you should be able to control your entire wireless network from a single interface and execute key processes to safeguard the environment and its users.

3 VERIFIED COMPREHENSIVE SECURITY

You need proof that your security solution defends your business against Wi-Fi attacks and can deliver on the following benefits:
- Provide automatic protection from the six known Wi-Fi threat categories
- Allow legitimate external access points to operate in the same airspace
- Restrict users from connecting to unsanctioned Wi-Fi access points

The Six Known Wi-Fi Threat Categories

"Evil Twin" AP

Neighbor AP

Rogue Client

Misconfigured AP

Rogue AP
Allows attackers to bypass perimeter security

Lures users to connect to it so as to spy on traffic, steal data and infect systems

Risks infection from connecting to other SSIDs while in range of the authorized AP

Delivers malware payloads to the network after connecting to malicious APs

Ad-Hoc Network
Uses peer-to-peer connections to evade security controls and risks exposure to malware

Opens networks to attack as a result of configuration errors

Miercom Wi-Fi Security Report

Test	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
	Detect	Prevent	Detect	Prevent	Detect	Prevent	Detect	Prevent
Rogue AP	P	P	F	N/A	F	MP	F	N/A
Rogue Client	P	P	F	N/A	F	MP	N/A	MP
Neighbor AP	P	P	P	P	F	N/A	F	N/A
Ad-Hoc Network	P	P	F	N/A	F	N/A	P	N/A
"Evil Twin" AP	P	P	P	F	P	MP	P	F
Misconfigured AP	P	P	P	N/A	N/A	N/A	N/A	N/A
Concurrent Threats	P	P	F	F	F	F	F	F

- P = Pass
- F = Fail
- MP = Marginal Pass
- N/A = Feature Not Supported

View the full Miercom report: **www.watchguard.com/wifi-security-report**

WatchGuard Secure, Cloud-Managed Wi-Fi

WatchGuard doesn't just offer Wi-Fi connectivity, we offer patented **security**, increased **productivity**, and improved **customer satisfaction**. When you deploy a WatchGuard access point that has WatchGuard Wi-Fi Cloud enabled, you unlock invaluable tools to take your business to the next level with industry-leading wireless security, engaging captive portals, location-based analytics engine, and centralized management.

Miercom verifies that WatchGuard is the only company to **automatically detect and prevent** the six known Wi-Fi threat categories.

WatchGuard®