



Harness the Power of a Secure and Reliable Wi-Fi Network Using the Trusted Wireless Environment Framework

56% of people connect to public Wi-Fi networks with **no password**¹

Internet of Things (IoT) connected devices worldwide are projected to amount to **30.9 billion units by 2025**²

Cybercriminals target the weakest link in the security chain

67% of people think public Wi-Fi is completely or somewhat safe – **43%** of those using public Wi-Fi had their online security compromised³

More than 50% of all cyberattacks are committed against SMBs – **60%** go out of business within 6 months of falling victim to an attack⁴

Cybercrime estimated to hit **\$8T in 2023**⁵

The 6 Known Wi-Fi Threat Categories Targeting Your Business

1. Evil Twin Access Point

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



2. Misconfigured Access Point

Opens networks to attack as a result of configuration errors.



3. Rogue Access Point

Allows attackers to bypass perimeter security.



4. Rogue Client

Delivers malware payloads to the network after connecting to a malicious access point.



5. Neighbor Access Point

Risks infection from connecting to other SSIDs while in range of the authorized access point.



6. Ad-Hoc Network

Uses peer-to-peer connections to evade security controls and risk exposure to malware.



Enabling a Trusted Wireless Environment can keep your business safe from all 6 known Wi-Fi threat categories.



Learn how WatchGuard's Trusted Wireless Environment framework can help you build a complete Wi-Fi network that is **fast, easy to manage**, and most importantly, **secure**.

www.watchguard.com/trustedwirelessenvironment



1. Data from Forbes
2. Data from Statista
3. Data from Forbes
4. Data from Cybersecurity Ventures
5. Data from Cybersecurity Ventures

*2023 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard logo are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGC67131_052223