WatchGuard

neuways

THE SIX KEY WIFI THREATS

More and more devices are leveraging **WiFi connectivity**. This trend isn't expected to slow down anytime soon, and while you, your customers, and employees demand access to fast WiFi, you might not know the huge gap it's leaving in your **security**.

Evil Twin Access Point

Misconfigured Access Point

Rogue Access Point

Rogue Client

Neighbour Access Point

Ad-Hoc Network

Is your **WiFi** protected?

What about the open **WiFi** network you connected to the other day in the coffee shop?

Or at the airport?

Crowded places and open **WiFi** networks are ideal locations for a hacker to take advantage of you and access your network.

More and more devices are leveraging **WiFi connectivity**. This trend isn't expected to slow down anytime soon, and while you, your customers, and employees demand access to fast WiFi, you might not be aware of the huge gap it's leaving in your **security**.

Evil Twin Access Point

Lures users to connect to it. Hackers can then spy on traffic, steal data, and infect systems.

Rogue Client

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

Misconfigured Access Point

Incorrectly configured WiFi access points can leave your network vulnerable to exploitation.

Neighbour Access Point

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

Rogue Access Point

Allows attackers to bypass perimeter security.

Ad-Hoc Network

Uses peer-to-peer connections to evade security controls and expose networks to malware.