# TrapAir

## Active WiFi Honeytraps


Generate realistic traffic and behaviour


**TrapAir uses Artificial Intelligence (AI) to create realistic, active hotspots that mimic your network. Any interaction with TrapAir alerts you that someone is trying to disrupt or connect to networks without permission.**

## Challenge

WiFi provides critical connectivity for our systems and users.

The problem with WiFi is security - it relies on mostly insecure protocols and standards, making it an easy target for interception.

Walls are not hard barriers for WiFi signals, allowing malicious and curious remote connection attempts from outside our homes and offices.

Your WiFi is not only attractive to data thieves, but also provides malicious actors a pathway to the internet. This can impact others and put your brand at risk.

It's almost impossible to review every anomalous connection attempt. Traditional monitoring tools also generate volumes of false alerts and require specialist knowledge to decipher.

## Solution

Each TrapAir creates an active, decoy WiFi hotspot. As legitimate users should not connect to random, untrusted networks, this means connections to TrapAir are rare and suspicious. This provides a high-fidelity warning that someone is attempting to connect to hotspots.

Our machine learning techniques ensure the traps appear active and realistic while all user activity is simulated.

TrapAir can be configured to watch and mimic your data and user behaviour. You can use our drop down menus to create traps based on the behaviour of your real WiFi network or our in-built libraries.

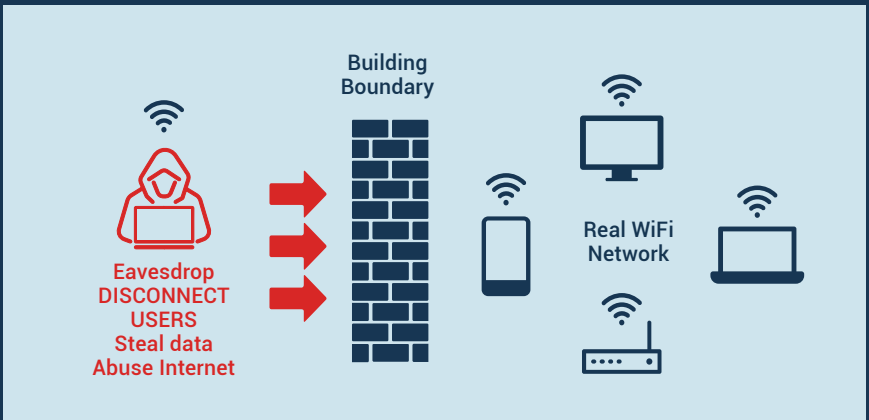
Your networks are always changing. TrapAir can be set to continually update its knowledge of your user behaviour and adjust the traps to match.

As a single device, TrapAir can detect connection attempts, plus nuisance activity that seeks to stop legitimate users from connecting.

Deployable multiple devices can also enable TrapAir to share information to help you locate the origin of connections.

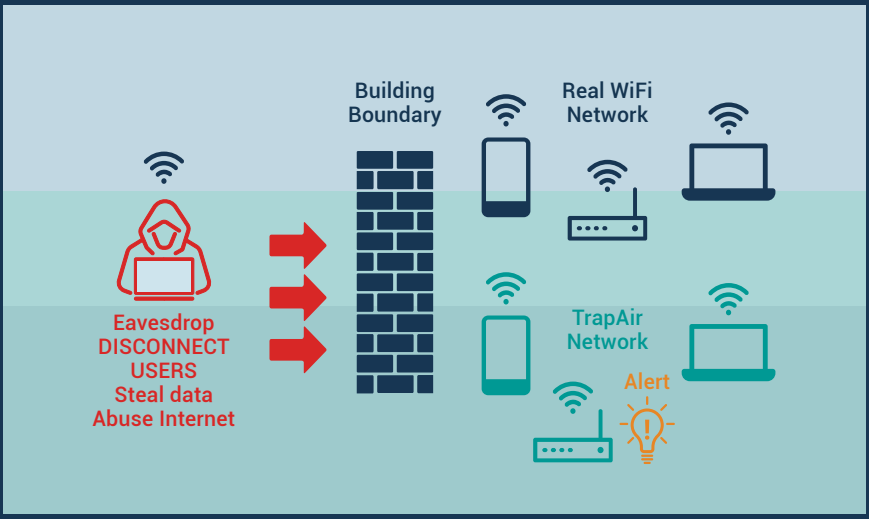
- Easy to set up
- Uncomplicated alerts
- Mimics your network activity
- Know when WiFi snoopers are nearby
- Locate the origin of malicious activity
- Fight back by wasting intruders' time

APPLIED AI




WiFi signals do not stop at our walls. This can allow curious and malicious behaviour such as eavesdropping, connection attempts and network disruption from beyond our building boundary.

This activity is hard to detect in busy office environments and among legitimate user errors and activity.




TrapAir uses AI to learn about real networks. It uses this learned information to create highly realistic, fake WiFi hotspots with active users. Any connections provide a warning that someone or something is looking to connect to WiFi networks in your vicinity.

TrapAir also wastes adversaries' time trying to find your real networks or attempting to crack your fake traffic.

## Technical Specifications

| | |
|---|---|
| **Deployment Options** | Single Device or Team Geolocation |
| **WiFi** | 802.11a/b/g/n/ac |
| **Power** | 802.3af PoE |
| **Dimensions** | 108 x 73 x 33 mm |
| **Weight** | 550g |
| **Management Access** | Any modern web browser |

## Operating Modes

| Colour | Activity |
|---|---|
| ● | Start up |
| ● | WiFi trap activated |
| ● | Learning |
| ● | Alert |
| ● | Error |

+61 2 6171 1111 / info@penten.com / www.penten.com
Penten @pentencyber