



AEGIS WIRELESS

WiFi Security Analysis Tool for Enterprise Endpoint Protection

Rylan Dansereau & Francesca Suarez-Leon

CIS 4951 - Capstone II | Spring 2026

Knight Foundation School of Computer & Information Sciences

FLORIDA INTERNATIONAL UNIVERSITY

Problem Definition

The surge in remote and hybrid work has created a critical gap in enterprise endpoint security. Employees connect daily from coffee shops, airports, and libraries through unvetted third-party networks outside corporate security perimeters.

58%

of U.S. workers with
remote-capable jobs
work hybrid or fully remote

45%

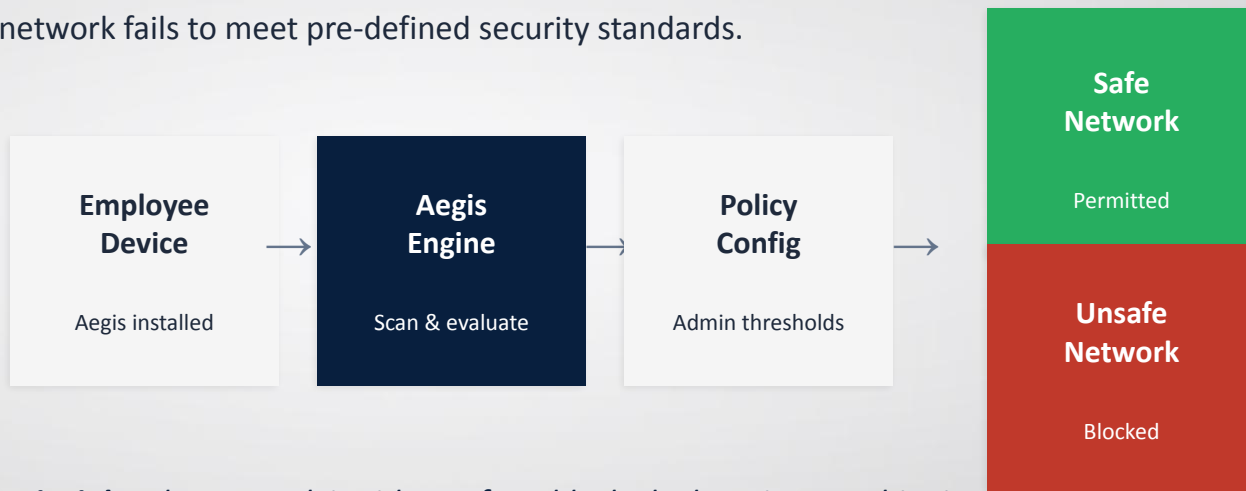
of breaches involve
compromised credentials
on unsecured Wi-Fi

\$4.9M

average cost of a
data breach
(IBM 2024)

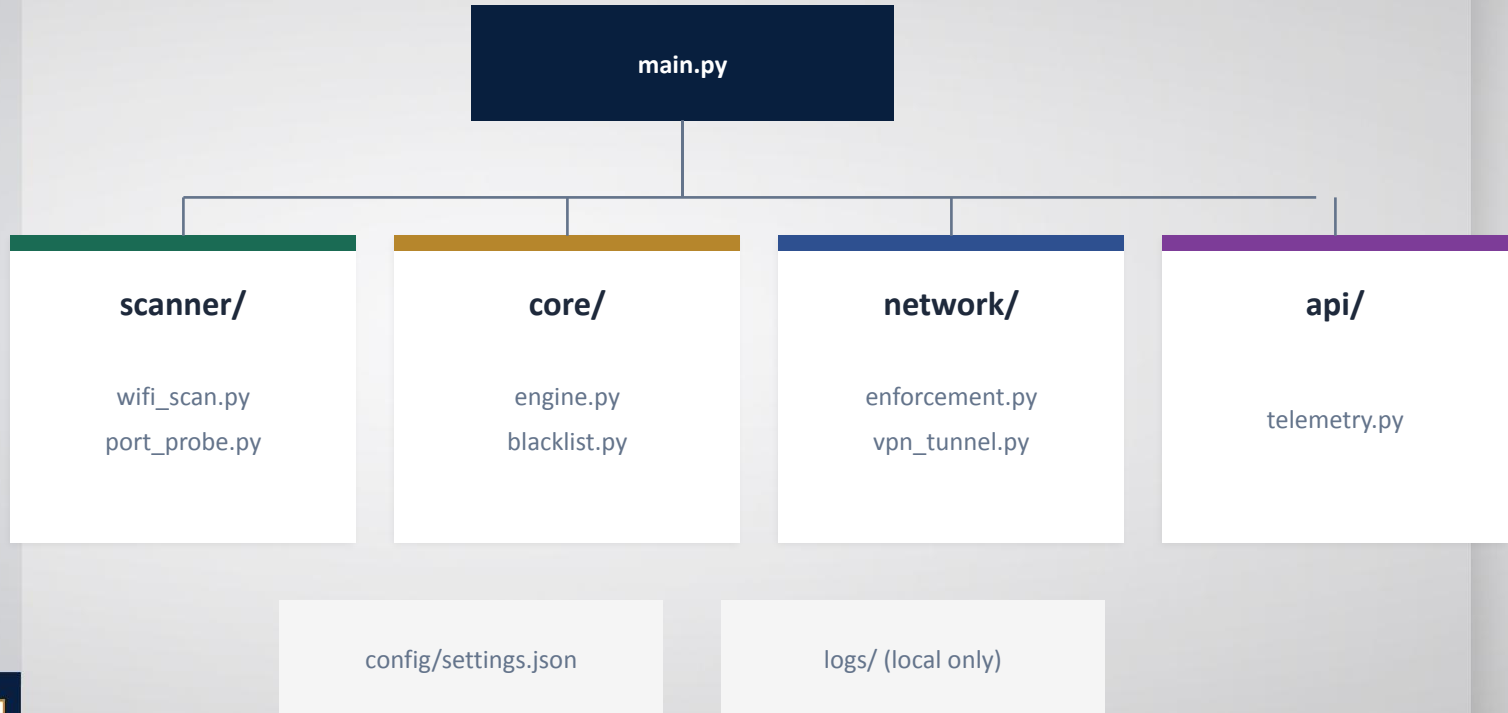
Solution: Aegis Wireless

Aegis Wireless is a Windows endpoint application that enforces network security policy by evaluating any Wi-Fi network an employee attempts to join — automatically blocking connection if the network fails to meet pre-defined security standards.



Key Principle: The network is either safe or blocked. There is no ambiguity.

System Architecture



Implementation & System Design

Platform

Python application using Windows Network Shell (netsh) commands for network discovery and metadata analysis.

User Interface

System tray background agent as well back pop up toast notifications.

Metadata Analysis

Passive scanning via netsh commands, collecting SSID, signal strength, encryption type, BSSID, and channel data.

Encryption Verification

Validates WPA2/WPA3 and rejects open, WEP, or misconfigured networks with configurable penalty scoring.

Policy Engine

JSON-based policy configuration defining minimum encryption standards, blocked network lists, and risk scoring parameters.

Audit Logging

All connection events, blocks, and approvals logged locally as timestamped .log and .json files for compliance review.

Key Features

Real-Time Blocking

Background agent scans at configurable intervals and auto-disconnects from dangerous networks.

Policy Driven

IT admins define acceptable security thresholds per organizational risk tolerance via JSON config.

Transparent UX

System tray with toast notifications. Employees see instant, plain-language status: safe or blocked.

Lightweight Agent

Runs silently on Windows startup via Registry Run key. No admin privileges required.

Encryption Verification

Validates WPA2/WPA3 and rejects open, WEP, or misconfigured networks automatically.

Audit Logging

All scan results, risk assessments, and enforcement actions saved locally and timestamped.

How It Works

1

Detect

The background agent scans for all nearby WiFi networks using OS-level commands, collecting SSID, signal, encryption, BSSID, channel, and band.

2

Scan

A multi-threaded port scanner probes the network for open TCP ports across 25 known services, identifying running services and capturing banners.

3

Evaluate

The risk engine scores each network 0 to 100 by running five checks: encryption strength, hidden SSID, dangerous ports, signal anomalies, and blacklist status.

4

Enforce

Dangerous networks are automatically blocked. The agent disconnects the device and notifies the employee via a system tray toast notification.

5

Log

All results, assessments, and enforcement actions are saved locally as timestamped .log and .json files for compliance review.

Testing & Evaluation

Test Scenario	Input	Expected	Result
Open WiFi detection	Open network (no encryption)	Score <= 60, MODERATE	PASS
WPA2 network	WPA2-encrypted network	Score = 100, SAFE	PASS
Blacklisted network	Previously flagged SSID	-50 pts, DANGEROUS	PASS
Dangerous port detection	Port 23 (Telnet) open	-8 pts per port	PASS
Auto-disconnect	DANGEROUS risk level	WiFi disconnected	PASS
Local logging	Any scan action	.log + .json created	PASS
VPN detection	VPN adapter present	Status: Active	PASS
Hidden SSID flagging	Network hiding name	-10 pts	PASS

Next Steps

Future Work

- MAC Address Anomaly Detection: track BSSIDs of known networks and flag potential evil twin attacks when the MAC changes
- Network Behavior Baseline: record normal port/device profiles and auto-flag deviations as potential intrusions
- MDM Integration: package for enterprise deployment via Intune or SCCM with centralized policy management
- Packet-Level Inspection: integrate Scapy for ARP spoofing detection and deep traffic analysis



Thank You

AEGIS WIRELESS

Rylan Dansereau & Francesca Suarez-Leon

CIS 4951 - Capstone II | Spring 2025

Instructor: Seyedmasoud Sadjadi