

Problem

The surge in remote and hybrid work has created a critical gap in enterprise endpoint security. Millions of Americans work daily from coffee shops, libraries, airports, and other public venues — connecting through unvetted third-party networks that fall entirely outside corporate security perimeters.

"How can companies allow Work from Home without incurring unnecessary risk from unsecured third-party networks?"

Prohibiting work outside designated networks is unrealistic. Enterprises refusing remote flexibility are rapidly losing top-tier talent, as hybrid and fully remote roles have become a baseline expectation for high-level candidates.

58%

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)

NETWORK THREAT LANDSCAPE

Threat	Risk	Impact
Evil Twin AP	HIGH	Credential theft, MITM
Unencrypted Traffic	HIGH	Data interception
Rogue DHCP	MED	Traffic redirection
Weak Encryption (WEP)	MED	Network key cracking
Open/No-Auth Network	HIGH	Packet sniffing

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.

Implementation & System Design

Key Features

How it Works

PLATFORM

Python application leveraging Windows Network Shell (netsh) commands for network discovery and validation.

METADATA ANALYSIS

Passive and active scanning via Windows Network Shell (Netsh) commands, combined with 802.11 frame inspection for encryption and AP validation.

POLICY ENGINE

JSON-based policy configuration, security policies are loaded from a local settings file, enabling IT admins to customize acceptable parameters per organizational requirements

USER INTERFACE

System tray application with toast notifications. Simple dashboard for IT admins to manage policy deployment and review event logs.

REAL-TIME BLOCKING

Windows 11 native application leveraging the Windows WLAN API for network event hooks and NativeWifi for adapter-level control.

POLICY DRIVEN

IT admins define acceptable security thresholds per organizational risk tolerance.

TRANSPARENT UX

Employees receive instant, plain-language status: safe or blocked — no guesswork..

LIGHTWEIGHT AGENT

Runs silently in the background on any Windows device with minimal resource usage.

ENCRYPTION VERIFICATION

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

AUDIT LOGGING

All connection events, blocks, and approvals logged for compliance review.

- 1

Detect: The background agent scans for all nearby WiFi networks
- 2

Scan: A multi-threaded port scanner probes the network
- 3

Evaluate: The risk engine scores each network from 0 to 100 by running multiple, configured security checks
- 4

Enforce: High risk networks are automatically blocked – No user action required
- 5

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

Summary & Impact

Aegis Wireless directly addresses the tension between workforce flexibility and enterprise security. By enforcing network-level policy at the endpoint — rather than relying on user judgment or VPN compliance — it removes third-party network vulnerability as an attack vector entirely. Enterprises adopting Aegis Wireless can confidently offer remote and hybrid work without expanding their attack surface, enabling them to attract top talent while maintaining security posture.

“Aegis gives companies clairvoyance over their remote endpoints — the network is either safe or blocked. There is no ambiguity.”

REFERENCES

[1] IBM Security. Cost of a Data Breach Report 2024. IBM Corporation.

[2] Pew Research Center. How Working From Home Has Changed. 2023.

[3] Microsoft. Windows WLAN API Documentation. Microsoft Docs, 2024.

[4] IEEE 802.11-2020. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[5] NIST SP 800-153. Guidelines for Securing Wireless Local Area Networks (WLANs).