IRONWIFI

WIRELESS GLOBAL CONGRESS · 2026

Everyone Is Talking About OpenRoaming.

Nobody Is Talking About This.

The Security Layer WiFi Never Had

From the OpenRoaming Standards Group co-chair.

Presented by Taylor Swanson · External Advisor, on behalf of IronWiFi

You have a WiFi security problem.

It's getting worse with the explosion of non-human identities.

A new identity layer is required.

THE BLIND SPOT

WiFi Without Identity Security = Open Attack Surface

IRONWIFI

WiFi TODAY — WITHOUT ITDR

- Credential abuse — **undetected**
- Identity anomalies — **invisible**
- AI agents — **unmonitored**
- Insider abuse — **hidden**
- Roaming abuse — **opaque**

WiFi + IronWiFi ITDR

- Credential abuse → **flagged**
- Identity anomalies → **detected**
- AI agents → **baselined**
- Insider abuse → **surfaced**
- Roaming abuse → **traced**

THIS LAYER DOES NOT EXIST IN THE WI-FI STACK TODAY

Existing vendors stop at authentication or observability — none operate at the identity-behavior layer at RADIUS.

Based on publicly available product information, as of 2026-05.

VENDORS REVIEWED

Cisco ISE · Fortinet · Juniper Mist

Aruba ClearPass · Microsoft Sentinel · Splunk

If a credential roams across continents in a minute — the identity layer is where you see it.

WiFi connectivity is built everywhere. The security layer is not.

IRONWIFI

Why This Layer Becomes Necessary Now

Four structural shifts make the identity-behavior layer inevitable.

Certificates Replacing Passwords

EAP-TLS adoption is accelerating. Certificate threats — expired, revoked, unknown CA, cert-user mismatch — are not visible to AD-centric ITDR.

Non-Human Identities Exploding

AI agents, automation, APIs, CI/CD pipelines, IoT controllers. All authenticate via RADIUS. None are governed at the identity plane today.

Federation Scale

OpenRoaming and Passpoint extend the identity surface across millions of hotspots. Blast radius for any compromised credential is now federation-wide.

SOC Shift to Identity-First

Zero Trust frameworks (NIST SP 800-207, CISA ZTMM) place identity behavior at the center. WiFi auth is the missing identity surface in those mandates.

This layer becomes necessary once identity is the control plane.

IRONWIFI

Where the Identity Layer Fits

WiFi stack today: no system evaluates identity behavior between auth and SOC.

ENTERPRISE & SOC
Splunk · Sentinel · QRadar · ServiceNow

IDENTITY LAYER (NEW)
IronWiFi ITDR · AI Agent Identity · Behavioral Baselines

NEW

FEDERATION & ROAMING
Passpoint · OpenRoaming · RoamingConsortium

AUTHENTICATION & POLICY
RADIUS · FreeRADIUS · Cisco ISE · ClearPass · NPS

WiFi INFRASTRUCTURE
Cisco · Aruba · Mist · Fortinet · Meraki · Ruckus · 70+ vendors

WHAT'S NEW

WBA V1.0.0 = prevention baseline (authentication, encryption, transport). The **detection layer** between auth and SOC — has not been built on WiFi.

WHERE IT SITS

- **Above RADIUS** — observes every auth and accounting signal.
- **Below the SOC** — feeds CEF / webhook detections upstream.
- **Alongside OpenRoaming** — additive, not corrective.

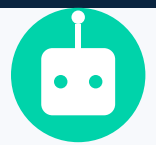
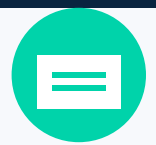
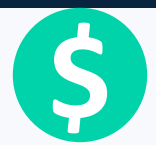
Reference: WBA Wi-Fi Security Guidelines V1.0.0, April 2026 — defines the prevention baseline.

Vendor names listed for context. Per public product information, as of 2026-05.

IRONWIFI

WiFi Identity Threat Detection and Response

First purpose-built threat detection for WiFi / RADIUS auth. · 60+ detection types across 8 engines — and growing.

Credential Attack	Identity Anomaly	Certificate Threat	Device Threat	Agent Anomaly	Portal Security	Insider Threat	Quota & Usage
							
Brute force Password spray Credential stuffing Replay & EAP downgrade	Impossible travel Time anomaly AP anomaly Frequency anomaly	Expired / revoked Unknown CA Mass issuance Cert-user mismatch	MAC spoofing Device cloning Rogue device Rapid MAC rotation	Rate spike New NAS / AP Cert change Off-hours New VLAN segment	Bot submissions Social-login abuse Session hijack Payment fraud Credential reuse	After-hours access Excessive roaming Privilege escalation Terminated user Concurrent sessions	Octet-volume exfil Bandwidth anomaly Dormant reactivation Trust-tag-scaled Charging anomaly

- Every detection mapped to MITRE ATT&CK.
- AI-driven behavioral baselines per identity (EMA).
- Automated response: CoA disconnect, VLAN quarantine, deny-list update.
- Shadow / Detect / Enforce modes — start safe, promote when confident.

IRONWIFI

What That Looks Like in Practice

Impossible Travel

User JFK (09:00) → SFO (09:45). Haversine limit exceeded.

MITRE T1078 — Valid Accounts

RESPONSE

Quarantine VLAN + alert SOC

Credential Stuffing

20+ failed auths for one User-Name across many MACs in 10 min, baseline-flagged.

MITRE T1110.004

RESPONSE

Alert SOC + CoA disconnect

MAC Spoofing

Same MAC on different NAS/APs in conflicting locations.

MITRE T1036.005 — Masquerading

RESPONSE

CoA disconnect unregistered device

Rogue AI Agent

LLM agent off-hours auth on new VLAN; baseline drops 2σ.

MITRE T1078.004

RESPONSE

Auto-quarantine + notify SOC

AI-GENERATED RESPONSE PLAYBOOKS

Every detection ships with a playbook — drop straight into your SOC runbook. No manual writing.

IRONWIFI

Network Identity for AI Agents

Anything using certificates + automation already behaves like an agent — CI/CD pipelines, API clients, bots, controllers.

AI agents are the next category, not the only one. Who registers them? Who detects when one goes rogue?

AGENT IDENTITY

- Certificate-based 802.1X auth.
- Purpose-scoped VLAN per agent type.
- Behavioral baselines + anomaly detection.
- Auto-quarantine via RADIUS CoA.

SHADOW AI DISCOVERY

- Detect unregistered agents in RADIUS traffic.
- 5 heuristics — confidence scored.
- Surface agents nobody deployed.
- Register before they become incidents.

IRONWIFI

What Your NOC Team Sees

Seven views of the IronWiFi management console — what your NOC sees in the live console.

DESIGN PARTNER PREVIEW

1

ITDR Dashboard

KPIs, threat timeline, risk distribution.

2

Incident Detail

Drill-down, MITRE technique, forensic context.

3

ITDR Settings

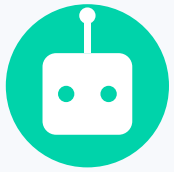
Engine cards, mode toggles, thresholds.

4

SIEM Integration

Provider selector, webhook, CEF preview.

5



Agent List

Registered agents — type, status, baseline.

6

Agent Detail

VLAN, behavioral events, quarantine.

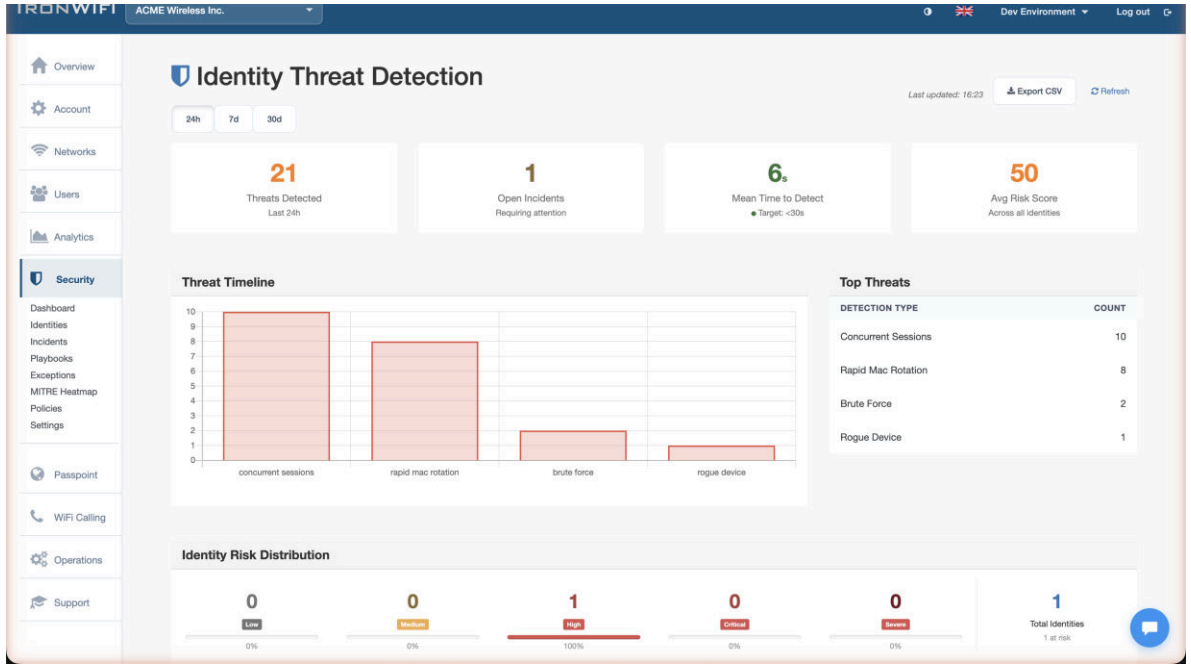
7

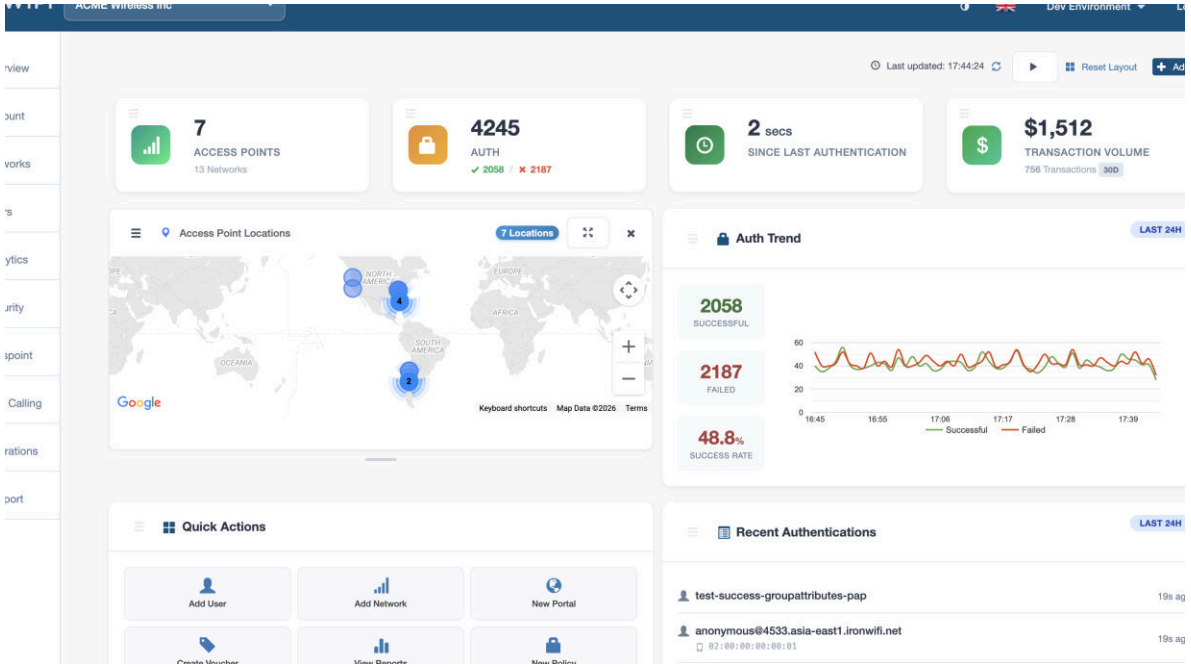
Shadow AI Discovery

Unregistered agents with confidence scores.

IRONWIFI

ITDR Dashboard

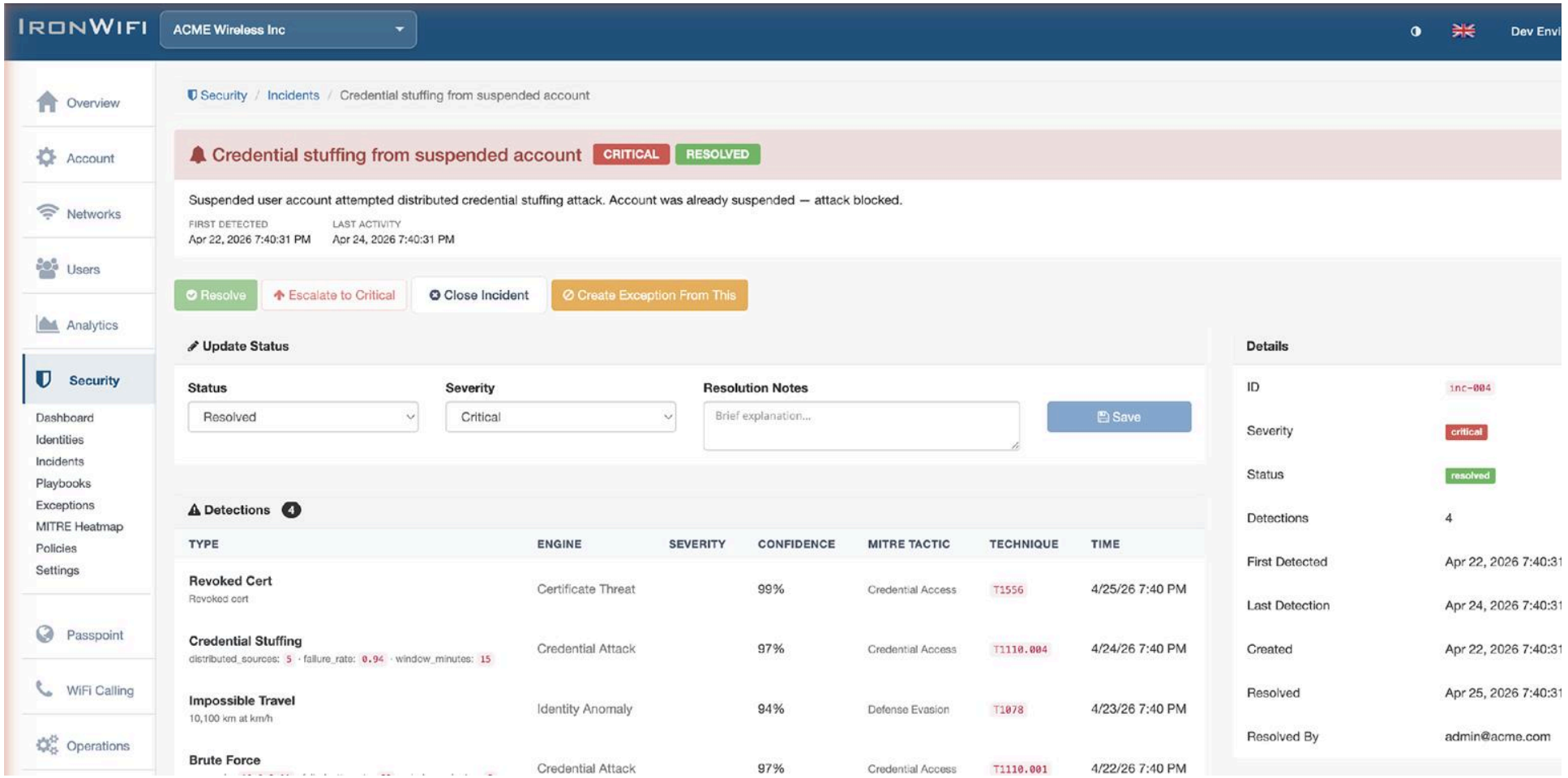




Real-time visibility into every identity-based threat on your WiFi network.

IRONWIFI

Incident Detail



Every incident mapped to MITRE ATT&CK with full forensic context.

IRONWIFI

Built on Production RADIUS Infrastructure

IronWiFi co-chairs the OpenRoaming Standards Group at the Wireless Broadband Alliance.

VENDOR-NEUTRAL	CLOUD-NATIVE	STANDARDS-ALIGNED	AUDITED	PATENT-PENDING
Cisco, Aruba, Mist, Fortinet, Meraki, Ruckus. 70+ supported.	**Multi-region on Cloud Spanner.** Carrier-grade async.	**RADIUS, 802.1X, EAP, Passpoint, OpenRoaming (settlement-free + settled).** SCEP, RADSEC.	**SOC 2 Type II audit completed.** Report issuance pending.	**8 patents pending.** ITDR · Agent ID · Trust-tag · Anomaly

- **Cloud RADIUS + PKI + Captive Portal + OpenRoaming** on one platform.
- Certificate-based auth via **SCEP** (Intune, Jamf, Google Admin).
- Built once, runs anywhere — your hardware, your federation.
- **ITDR and Agent Identity** sit on top — the layer this room is missing.

Vendor names listed for context. Per public product information, as of 2026-05.

IRONWIFI

What This Enables

Carriers — Federation Security

Credentials roam across OpenRoaming. We flag "impossible-travel" and reuse patterns that local hotspots miss.

Enterprises — Multi-Site Campus

Cloud-native certificate auth for any access point. Cisco, Aruba, Mist, Meraki—managed in one console.

Venues — IoT & AI Agents

Treat IoT and AI agents as identities. Govern with scoped access and discover unauthorized shadow AI.

IRONWIFI

Two Categories. One Missing Layer.

Every vendor in this category does one of two things. **Nobody evaluates identity behavior at the network layer.**

Based on publicly available product information, as of 2026-05.

AUTHENTICATE: ACCESS CONTROL

Cisco ISE
On-prem campus identity. No multi-vendor cloud roaming, no WiFi ITDR.

Aruba ClearPass
Policy + AAA. Not behavioral baselines or MITRE detection.

Fortinet NAC
Network admission control. Not identity threat detection.

OBSERVE: POST-EVENT LOGGING

Juniper Mist
AI-driven WiFi assurance. Network ops, not identity-plane detection.

Microsoft Sentinel
SIEM that ingests events. Not the source of WiFi detections.

Splunk Enterprise Security
SIEM and SOAR. Consumes detections — does not generate WiFi-identity ones.

ZERO TRUST = IDENTITY + ACCESS + BEHAVIOR

IDENTITY	ACCESS	BEHAVIOR
Microsoft · Okta	Cisco · Aruba (NAC)	IronWiFi (ITDR)

All three are required. Remove one, and you get a blind spot.

IRONWIFI

Six Ways to Plug Into the Security Layer

COMMERCIAL ENGAGEMENT

OEM

Embed identity layer in your hardware.

For: AP & gateway vendors

WHITE-LABEL

Offer ITDR under your brand.

For: MSSPs & carriers

CARRIER INTEGRATION

Usage-based pricing at carrier scale.

For: Tier-1 / Tier-2 MNOs

TECHNICAL INTEGRATION

FEDERATION SECURITY

Identity threat detection across OpenRoaming.

For: WBA contributors

AI AGENT IDENTITY

Identity for the non-human workforce.

For: AI platforms & enterprises

SOC INTEGRATION

CEF + webhook to Splunk, Sentinel, Elastic.

For: SOC / SIEM teams

Pick your path. The next slide shows where to start.

Patent-pending architecture · 8 patents pending

DESIGN PARTNER PROGRAM

IRONWIFI

Limited Partner Slots Open for Q3 2026

WHAT WE PROVIDE

- WiFi ITDR — full deployment
- Agent Identity + Shadow AI
- AI-generated playbooks
- Dedicated engineering support
- Zero cost during the program

WHAT WE NEED

- Real federation traffic
- Access to RADIUS auth flows
- Feedback on detection tuning
- Joint case study post-launch
- 90-day evaluation window

WHAT YOU GET

- First-mover access
- Influence on product roadmap
- Locked-in pricing at GA
- Joint go-to-market
- Security layer competitors lack

wgc2026@ironwifi.com · meetings.ironwifi.com/#/wgc2026

IRONWIFI

Questions?

The Security Layer WiFi Never Had

wgc2026@ironwifi.com

meetings.ironwifi.com/#/wgc2026

SCAN TO SCHEDULE

meetings.ironwifi.com/#/wgc2026

IRONWIFI

LET'S BUILD THIS TOGETHER

Every WiFi network already trusts identities. None of them verify behavior. That is the layer we're building.

IronWiFi Team

Sales & Partnerships

wgc2026@ironwifi.com

SCAN TO SCHEDULE

meetings.ironwifi.com/#/wgc2026

Direct to the IronWiFi partnerships team

Presented by Taylor Swanson · External Advisor