Wireless Security Assessment – Complete RF Visibility, Zero Invisible Gaps

A Strategic Briefing for CISOs, CTOs, Network Architects, IT Infrastructure Leads, and Facilities Managers. Wireless networks have become the default connectivity layer for employees, guests, IoT devices, and building systems.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled

WSA

Wireless Security Assessment

Understanding Wireless Security -
The Risks Organizations Often Overlook

Wireless networks create convenience, mobility, and efficiency. They also create an invisible attack surface that **most security tools cannot see.**

88%

Organizations With At Least One Wireless Vuinerability

Most are configuration paps, not exotic exploits — rogue APs, wook PSKs, and misconfigured 802.1X deployments top the list.

40%+

Enterprise Assessments Where Rogue APs Are Found

Mony are deployed by employees for convenience. Some are planted by adversories. Both create the some exposure.

258

Average Breach Lifecycle (Days)

Wireless compromises rank among the hardest to detect — minimal trace in endpoint monitoring and most SIEM configurations.

$4.88M

Global Average Breach Cost

Credential horvest via evil twin or PMKID capture can serve as the initial access vector for a breach that escolates well beyond the wireless layer.

Key Insight: The consistent pattern across wireless incidents is not sophisticated tooling — It is the absence of dedicated RF visibility. Firewalls, endpoint detection, and NAC solutions do not observe the wireless loyer. That gap is what a structured wireless assessment closes.

Common Wireless Threats That Create Real Business Risk

Rogue Access Points

Unauthorized APs operating undetected for months inside enterprise environments

Weak PSKs

Pre-shared keys vulnerable to offline passphrase crocking via PMKJD capture

Misconfigured 802.1X

EAP deplayment errors enabling credential interception and bypass

RF Blind Spots

Bluetooth, BLE, Zigbee, and industrial RF protocols operating without visibility

Evil Twin APs

Replicated SSIDs and BSSIDs invisible to users and most SIEM platforms

Unvalidated Segmentation

Wireless-to-wired lateral movement paths not tested under active attack conditions

Five Misconceptions We Hear Every Week

These are not misconceptions to correct. They are reasonable assumptions that need updated context.

What You Think	The Reality
We upgraded to WPA3, so our wireless security is solid.	WPA3 addresses WPA2 weaknesses but introduces the Dragonblood vulnerability class. Downgrade attacks can force clients to WPA2. Configuration arrors and client-side weaknesses still apply.
Rogue access points would be obvious — someone would notice.	Evil twin attacks replicate the exact SSID, BSSID, and signal strength of your legitimate APs. Without dedicated wireless IDS, they are invisible to users and most SIEM platforms.
Our NAC solution handles unauthorized wireless connections.	NAC validates device identity at connection time. It does not detect passive reconnaissance, PMKID capture, rogue AP deployment, or RF-layer attacks. These require purpose-built wireless assessment.
Wireless attacks require proximity, so they are lower risk.	Directional antennas sustain attack sessions from 500 to 1,000 meters. Adversaries target offices from parking areas and adjacent buildings routinely. Proximity is not a meaningful control in urbon environments.
Bluetooth is short-range and low risk.	Class 1 Bluetooth operates at 100 meters. BLE advertisements are passively scannable without pairing, BlueBorna, BLESa, and BIAS vulnerabilities have affected billions of enterprise devices.

What We Assess Across Your Wireless Environment

A complete view of your wireless attack surface — across protocols, devices, and environments. Because **what you can't see, attackers can**.

500m
Attack Range
Directional antennas can sustain attack sessions from 500 to 1,000 meters beyond your perimeter.

WPA3
Not a Sliver Bullet
Dragonblood vulnerabilities, downgrade attacks, and configuration errors still create real risk.

3–5
Devices Per User
BYOD and personal devices expand your wireless attack surface significantly.

BLE
Passively Scannable
BLE beacons and advertisements are visible without pairing — steafih by design.

Every Layer
Needs Validation
From Wi-Fi to industrial RF — each layer must be tested, not assumed secure.

Six Layers. Zero Assumptions.

Our Wireless VAPT methodology evaluates every layer of your RF ecosystem with active testing.

Layer	What We Assess	Risk Without Assessment
Wi-Fi Infrastructure	WPA2/WPA3, 802.1X/EAP, PSK strength, captive portal, deauth resistance, PMKID capture	Credential theft, weak configurations, offline passphrase cracking
Rogue AP & Evil Twin	Unauthorized AP detection, evil twin deployment, BSSID cloning, honeypot validation	Rague / malicious APs operate undetected for months
Bluetooth & BLE	Device enumeration, BlueBorne, BLESa, BIAS testing, poiring hypass	Medical, building, and user devices exposed to known CVEs
RF Protocols	Zigbee, Z-Wave, RFID, LoRa, NFC, and industrial RF protocol analysis	Legacy protocols connect to production networks with no authentication
Client Device Posture	Auto-connect behavior, saved profiles, captive portal bypass, client-side vulnerabilities	Endpoints sliently join malicious networks or leak credentials
Network Segmentation & Access Control	Wireless-to-wired segmentation, ACL validation, lateral movement testing	Attackers pivot from wireless into core networks without restriction

Compliance Frameworks That Require Wireless Security Controls

Regulatory expectations are clear — wireless security is no longer optional.

PCI DSS 4.0
Quarterly wireless scans and roque AP detection mandatory (Req. 11.2)

ISO 27001:2022
Wireless network controls under Annex A.8.20 and A.8.21

HIPAA
Security Rule requires encrypted wireless transmission and access control for PHI

NIS2 / GDPR
Network security controls for personal data — wireless explicitty in scope

RBI / SEBI / MAS
Wireless governance and access controls required for regulated entities

Wireless VAPT Investment (single enterprise site): a fraction of the average breach cost.
Average wireless-originating breach: $4.88M – $9.77M depending on sector.

Current State vs. Future State –
From Invisible Risk to Measurable Resilience

A tested wireless security program eliminates blind spots, reduces business risk, and strengthens your security posture across the enterprise.

Current State	Future State
Without Dedicated Wireless Assessment	**With Structured Wireless VAPT Program**
Limited Visibility Wireless inventory based on assumptions. Rogue APs and unauthorized devices may be active.	**Complete RF Visibility** All authorized and rogue APs, clients, and RF devices are discovered and documented.
Credential Exposure WPA2 PMKID captures and weak PSKs can be cracked offline without leaving log traces.	**Hardened Authentication** WPA2/WPA3 configurations validated. PMKID resistance confirmed. Strong PSK and EAP controls enforced.
Unmapped RF Risks Bluetooth, BLE, Zigbee, and industrial RF assets remain unquantified and unmonitored.	**Full RF Attack Surface Mapping** Bluetooth, BLE, Zigbee, RFID, and industrial RF risks identified with prioritized remediation.
Untested Segmentation Wireless-to-wired lateral movement paths are not validated under attack conditions.	**Segmentation Validated** Wireless-to-wired boundaries and ACLs tested to prevent lateral movement and privilege escolution.
Compliance Uncertainty PCI D55 quarterly wireless scan and other regulatory requirements may not be formally met.	**Compliance Confidence** PCI DS5, ISO 27001, HIPAA, GDPR, and other requirements met with evidence-backed reports.
Higher Financial Impact Undetected wireless attacks lead to higher breach likelihood, financial less, and reputational damage.	**Lower Risk. Lower Cost.** Reduced breach likelihood, lower insurance premiums, and stronger stakeholder trust.

The Business Impact of Proactive Wireless Security

Investment in wireless security today prevents significant financial and operational impact tomorrow.

$4.88M – $9.77M
Average Breach Cost
Wireless-originating breaches cost millions across industries.

20 – 40%
Insurance Premium Reduction
Documented wireless VAPT evidence reduces cyber insurance premiums.

15 – 80x
Return on Security Investment
Wireless VAPT delivers significant ROI compared to potential breach costs.

Operational Continuity
Secure wireless means uninterrupted business operations and protected customer trust.

Final Thought: Wireless threats are real, measurable, and preventable.
Visibility today. Resilience tomorrow.

Choosing the Right Partner –
Why Briskinfosec for Wireless Security

A partner who tests the full RF layer, maps findings to your compliance posture, and helps you improve — not just delivers a report.

Capability	Typical Assessment Firms	Briskinfosec Advantage
Accreditation & Trust	Self-certified or limited scope	**CREST Approved** – India's ONLY globally, CERT-In Empanelied, and ISO 27001:2022 Certified.
RF Coverage	Wi-Fi only or Wi-Fi + Bluetooth	**Full spectrum assessment:** Wi-Fi, Bluetooth, BLE, Zigbee, Z-Wave, RFID, and industrial RF protocols.
Attack Simulation	Configuration review only	**Live attack simulation** including evil twin deplayment, PMKID capture, segmentation bypass attempts (scoped & controlled).
OT / ICS Wireless	Out of scope	**IT-OT wireless boundary testing,** industrial RF protocol assessment, and PLC-connected wireless evaluation.
Compliance Mapping	One or two frameworks	**PCI DSS, ISO 27001, HIPAA, GDPR, NIS2, RBI, SEBI, MAS** — mapped to every finding with audit-ready evidence.
Scoring & Maturity	Finding list only	**bSAFE wireless maturity score** across 7 layers and 73 controls with prioritized remediation roadmap.
Post Assessment Support	Report delivered, engagement closed	**LURA portal** for tracking, reassessment scheduling, and continuous monitoring integration with bSOC.

Our Methodology. Your Assurance.

Plan & Scope ▸ Discover & Map ▸ Assess & Exploit ▸ Analyze & Score ▸ Report & Remediate ▸ Revalidate & Monitor

Our Track Record. Your Due Diligence.

Published outcomes from our security assessment program ccross 20+ countries.

540+ Clients Across 20+ Countries

4800+ Security Assessments Delivered

0% Client Breach Rate Post-Engagement

99.8% Compliance Achievement Rate

Briskinfosec is **India's ONLY CREST Approved** security assessment company, delivering global-standard methodology with local expertise, advanced tooling, and actionable reporting that drives real improvement.

Our Engagement Tiers –
Choose What Fits Your Security Journey

Each tier delivers independent value. Most organizations begin with a Wireless Vulnerability Scan and expand to a continuous program for maximum protection.

01

Wireless Vulnerability Scan

Rapid identification of authorized and rogue APs, misconfigurations, and exposed wireless assets. Includes risk prioritization and actionable recommendations.

Typical Timeline
1 Week

02

Full Wireless VAPT

Comprehensive assessment of Wi-Fi, Bluetooth, BLE, and RF protocols with active attack simulation, segmentation testing, and bSAFE wireless maturity scoring.
Includes compliance evidence package.

Typical Timeline
2 – 3 Weeks

03

Wireless Continuous Monitoring

Dedicated wireless IDS integrated with bSOC 24/7 monitoring for real-time rogue AP detection, anomaly alerts, and proactive threat response.

Ongoing Program

04

Annual Wireless Program

Recurring assessment on your compliance calendar with maturity tracking, reassessment, and updated evidence packages for auditors and regulators.

Annual Program

What You Get Across All Engagements

- Actionable Risk Prioritization
- Executive Summary
- Technical Report
- Remediation Roadmap
- Compliance Evidence
- Expert Support

Share These 8 Details.
Receive a Tailored Scope Within 48 Hours.

1. Organization Name _____
2. Industry Vertical _____
3. Number of Sites or Locations to Assess _____
4. Approximate Number of Access Points Per Site _____
5. Wireless Protocols in Use
   (Wi-Fi Only / Bluetooth / BLE / Zigbee / RFID / Industrial RF) _____
6. Current Wireless Security Controls
   (NAC / Wireless IDS / 86Z.1X / PSK / None) _____
7. Primary Compliance Requirement Driving This Assessment
   (PCI DSS / ISO 27001 / HIPAA / Internal Audit) _____
8. Preferred Assessment Timeline _____

The right visibility today prevents the invisible from becoming irreversible tomorrow.

Assess. Remediate. Assure. Stay Ahead.

What Happens Next?

Client Breaches
Post-assessment security record

Start With Zero Commitment

Understanding your unique security challenges begins with a conversation. We offer a no-obligation consultation to assess your current posture and identify immediate risk areas.

Our Team Holds Industry-Leading Certifications

We invest heavily in our team's continuous education because the threat landscape never stops evolving. Neither do we.

OSCP | OSWE | CISSP | CISA | CEH

CREST Accredited
Internationally certified penetration testing excellence

CERT-IN Empanelled
Government-recognized trusted cybersecurity assessment provider

ISO 27001 : 2022 Certified
Our own security practices are independently audited and verified annually

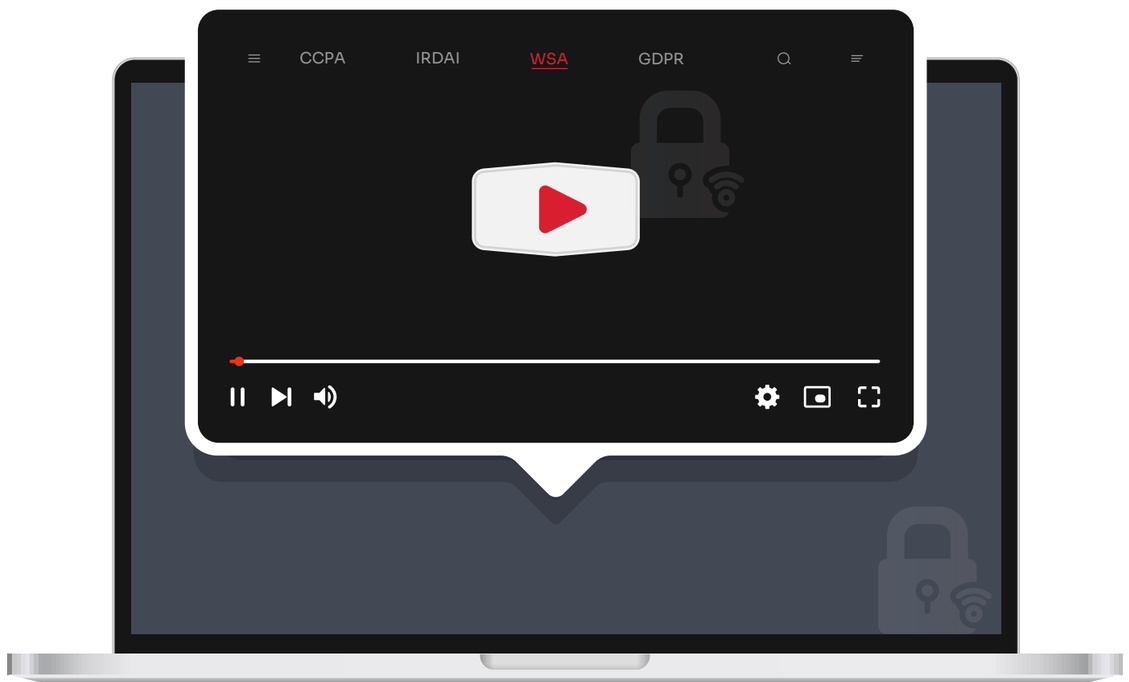
25+
Countries Client Portfolio

67%
Logic flaws missed by bots

98%
Client retention

640+
Successful Customers

5600+
Delivered in 24 countries



Reach us for FREE
consultation

Book Now

sales@briskinfosec.com
www.briskinfosec.com

Our Geographical Presence India UAE