HUIJUE GROUP

Open RAN After Huawei: More Vendor Choice or More Software Supply-Chain Risk?

Open RAN can reduce dependence on one integrated radio supplier, but it also moves more security and integration responsibility into software, cloud infrastructure and the operator's own processes. The real choice is not openness versus security. It is which risks the buyer is prepared to see, test and own.

OPEN RAN SECURITY

Open RAN After Huawei: More Vendor Choice or More Software Supply-Chain Risk?

Open RAN can reduce dependence on one integrated radio supplier, but it also moves more security and integration responsibility into software, cloud infrastructure and the operator’s own processes. The real choice is not openness versus security. It is which risks the buyer is prepared to see, test and own.

Updated August 4, 2026
Buyer and network-security guide
Approx. 18-minute read

Open RAN guide
Short answer
Four different ideas
How the risk map changes
Architecture and ownership
Security benefits
Software supply-chain risks
After Huawei
Worked patch incident
RFP evidence
Integration test plan
Contract boundaries
Decision framework

Open RAN Redistributes Risk

Suppose a mobile operator is required to replace Huawei radio-access equipment. Open RAN appears to offer a clean answer: buy the radio unit from one company, the distributed and centralised units from another, run them on a third party’s cloud, and choose software applications independently.

That architecture can widen the field of suppliers and reduce the consequence of one vendor controlling the whole RAN. It can also expose interfaces that were previously internal, add software packages from several development organisations and leave the operator coordinating patches across products with different release cycles.

So, does **Open RAN after Huawei** provide more vendor choice or more software supply-

chain risk? In practice, it does both. Vendor concentration risk may fall while integration, application, cloud and lifecycle-governance risk rise. Whether total risk improves depends less on the number of logos and more on five operating capabilities:

- the ability to identify every delivered hardware and software component;
- the authority to control identities, certificates, signing keys and privileged access;
- a lab that can reproduce the production stack and test multi-vendor changes;
- contracts that assign incident, patch and end-of-life responsibility; and
- an operator or prime integrator capable of resolving faults across organisational boundaries.

This is a technical and procurement framework, not a legal opinion. National restrictions, public-funding conditions and operator security obligations differ. A named-vendor exclusion should be checked against the current rule and the exact network function being purchased.

Do Not Treat Four Different Ideas as Synonyms

Many Open RAN discussions become confused before the security review starts. Four related ideas are often compressed into one word: open.

Idea	What it means	What it does not guarantee
Open interfaces	Components communicate through published, standardised specifications	Correct implementation, secure configuration or interoperability in every feature combination
Disaggregated RAN	Radio, baseband functions, cloud infrastructure and management can be separated	That the operator will actually buy them from different suppliers
Vendor diversity	More than one supplier can compete for a layer or role	Independence if several vendors share the same chipset, code library, cloud platform or subcontractor
Open-source software	Source code is available under an open-source licence	That deployed code is reviewed, reproducible, maintained or free of vulnerable dependencies

An operator can deploy O-RAN interfaces with proprietary software throughout. It can also purchase an apparently multi-vendor system in which one integrator selects every component and controls the management plane. Conversely, a conventional RAN may contain open-source dependencies without exposing an open interface to the buyer.

This distinction matters in a security questionnaire. Asking whether a product is “Open RAN compliant” does not reveal who compiled the binary, who signed the container image, which third-party packages it contains or how an xApp receives permission to

influence radio behaviour.

From a Sealed Supply Chain to a Visible One

A traditional single-vendor RAN is not simple in an absolute sense. It contains operating systems, chipsets, libraries, build systems, remote-support tools and subcontractors. Much of that complexity is simply hidden behind one commercial and technical boundary.

Open RAN moves several boundaries into view. That is not automatically a weakness. Visibility creates an opportunity to test interfaces, compare implementations and replace a component without replacing the entire stack. Yet the buyer must now govern what the integrated vendor previously governed internally.

The US National Telecommunications and Information Administration reached a useful, measured conclusion in its 2023 assessment. Most analysed threats affected both traditional and Open RAN; only 4% of the threats studied were considered unique to Open RAN. The report also found that the attack surface could increase to a small degree and that multi-vendor coordination becomes harder. At the same time, open specifications can improve testing and visibility. The NTIA Open RAN Security Report page is worth reading because it avoids both the claim that openness is inherently unsafe and the claim that standards remove operational risk.

Risk area	Integrated single-vendor RAN	Multi-vendor Open RAN
Supplier concentration	High dependency on one product roadmap and support organisation	Potentially lower, if components are genuinely substitutable
Interface security	Many internal interfaces are proprietary and less visible to the operator	More exposed, documented interfaces require identity, authorisation and configuration control
Fault ownership	One vendor normally owns end-to-end diagnosis	Faults can cross radio, cloud, transport, orchestration and application contracts
Software provenance	Buyer depends heavily on one vendor’s internal assurance	Buyer can demand evidence per component, but must correlate several evidence sets
Patch coordination	One release train, with the risk of vendor delay	Several release trains, compatibility windows and rollback paths
Substitution	Large replacement boundary	Smaller replacement boundary in theory; integration retesting remains necessary

The honest description is therefore not “closed is secure” or “open is secure.” A closed architecture concentrates trust. An open architecture distributes trust and makes its

management a first-order engineering task.

Where Software Supply-Chain Responsibility Sits

An Open RAN security review should follow the software and control paths, not stop at the O-RAN fronthaul label. A typical deployment may involve the following layers:

Layer or function	Typical security question	Evidence to request
O-RU	Can unauthorised firmware or configuration reach the radio unit?	Secure-boot description, signed firmware process, device identity and rollback method
O-DU and O-CU	Are workloads isolated, hardened and traceable to approved builds?	Image digest, software bill of materials, hardening profile and vulnerability history
O-Cloud	Who secures Kubernetes, virtualisation, accelerators, hosts and the image registry?	Shared-responsibility matrix, platform configuration baseline and privileged-access records
SMO	Can one compromised management identity modify a large part of the network?	Role model, MFA, audit logging, certificate lifecycle and backup restoration test
Non-RT RIC and rApps	What data can each application read, and what policy can it change?	Permission manifest, onboarding checks, data-flow map and application revocation procedure
Near-RT RIC and xApps	Could an application make unsafe near-real-time control decisions?	Authorisation limits, conflict handling, performance guardrails and kill switch
CI/CD pipeline	Can source, dependencies, build runners or signing steps be altered?	Build provenance, protected branch policy, signing-key controls and reproducible-build evidence
Remote support	Can a supplier enter production without operator approval or usable logs?	Named access path, just-in-time approval, session recording and emergency-access procedure

The O-RAN ALLIANCE security architecture treats the environment as zero trust: components and users should be authenticated and authorised continuously, communications protected, and security events logged. Its 2026 update also calls for a vendor-signed, NTIA-compliant SBOM with each software delivery and describes alignment work with the GSMA Network Equipment Security Assurance Scheme. These are meaningful controls, but a published specification is not evidence that a particular product, build or operator deployment implements it. See the O-RAN ALLIANCE Security Update 2026 for the current standards direction.

Where Open RAN Can Improve Security

Security teams sometimes discuss Open RAN only as an expansion of attack surface. That misses several practical advantages.

Specifications make claims testable

A documented interface gives an independent lab a target. Teams can test malformed messages, certificate handling, authorisation decisions and failure behaviour without first reverse-engineering a proprietary protocol. Openness does not ensure a correct implementation, but it can make a weak one easier to identify.

Component replacement can reduce strategic lock-in

If a supplier stops maintaining a product, becomes restricted or fails commercially, a well-conformed component may be replaced within a defined boundary. The qualifier matters. Substitution is credible only where profiles, optional features, performance and management behaviour have been tested with more than one implementation.

Cloud tooling can shorten some security operations

Immutable images, automated policy checks, staged deployment and rapid rollback can improve patch discipline. They also create a concentrated pipeline that must be protected. An automated delivery system is an advantage when it is controlled; it becomes a fast distribution mechanism for a bad build when it is not.

Telemetry can reveal cross-layer behaviour

Open management and control interfaces can give an operator better information about configuration, workload health and application actions. Good observability shortens incident investigation. It also creates sensitive operational data that needs access limits, retention rules and integrity protection.

Supplier diversity can improve negotiating and continuity options

Competition at separate layers may reduce reliance on a single commercial roadmap. It can also let an operator choose a specialist security or integration service. The benefit disappears if nominally separate suppliers depend on the same unsupported library, hosted build service or sole hardware accelerator. Diversity must be measured below the brand level.

The Software Supply-Chain Risks That Deserve More Attention

The most important Open RAN risks are not dramatic backdoors invented for a slide deck. They are ordinary software-management failures operating at network scale.

An SBOM can be present and still be unusable

A software bill of materials is a component inventory, not a security certificate. It helps answer which package and version may be affected by a disclosed vulnerability. It does not prove that the component is reachable, correctly configured, patched or free from an unknown flaw.

Buyers should request an SBOM in a machine-readable format, tied to the exact release and signed by the supplier. They also need a process that maps new vulnerability notices to deployed assets and records the supplier’s exploitability assessment. NIST describes an SBOM as a formal record of software components and their relationships, and recommends integration with vulnerability and risk-management processes. Its software supply-chain guidance explains the intended use more accurately than treating an SBOM as a compliance attachment.

Application onboarding can become the new vendor gate

xApps and rApps are often presented as a route to faster innovation. That is plausible, but each application introduces code, dependencies, permissions and a support lifecycle. The onboarding process should verify package signatures, declared permissions, interface use, data access, resource limits, vulnerability status and rollback. An application should not receive network-wide privileges simply because it passed functional testing.

Certificates can fail quietly

Open interfaces rely heavily on digital identity. Certificates expire, private keys leak, clocks drift and revocation mechanisms are sometimes untested. Procurement teams should ask who operates the public-key infrastructure, how factory identities are enrolled, whether a supplier can create production credentials and what happens when a root or intermediate certificate must be replaced across live sites.

The O-Cloud can create correlated failure

Disaggregation at the RAN layer may coexist with concentration at the cloud layer. A shared Kubernetes platform, container registry, accelerator driver or orchestration tool can affect several vendors at once. The operator needs an architecture-level dependency map, not separate product security statements that never identify common infrastructure.

Patch compatibility can delay a sound fix

A supplier may publish a security update promptly, yet the operator cannot deploy it

until adjacent components have been regression tested. Long compatibility chains create exposure windows. Tender documents should therefore define severity-based notification and remediation targets, but also require emergency mitigations and supported compatibility matrices.

AI and optimisation software can alter radio outcomes

RIC applications may use models to optimise handover, energy use or traffic behaviour. Buyers should identify the source and ownership of training data, model version, update authority, performance boundaries and fallback mode. A model can be intact and still make poor decisions when the operating environment changes. Monitoring must therefore cover behaviour, not only file integrity.

What Changes When Open RAN Follows Huawei?

The phrase “after Huawei” can describe several very different projects: a government-mandated removal, an operator’s supplier-diversification plan, an end-of-support replacement or a new network designed to avoid future concentration. The project motive changes the schedule and the acceptable risk.

Removing one supplier does not automatically create diversity. An operator may replace Huawei with another end-to-end prime contractor and retain almost the same concentration model. Alternatively, it may procure multiple Open RAN components but allow one integrator to control the O-Cloud, SMO, signing infrastructure and support access. The logo count rises while the operational control point remains concentrated.

Nor should country of origin be used as a substitute for product evidence. Policy restrictions must be followed where they apply, but technical assurance still requires architecture, provenance, access and lifecycle evidence from every permitted supplier. A European or American label does not make a vulnerable dependency harmless; Chinese manufacture does not by itself prove malicious behaviour. The related guide on white-label telecom equipment and procurement restrictions explains why the producer, firmware and support chain matter more than the badge.

Before selecting an Open RAN replacement, the operator should inventory what the outgoing integrated vendor currently supplies beyond radio hardware:

- network management and performance data;
- configuration history and accepted parameter ranges;
- timing and transport dependencies;
- alarm correlation and fault-resolution procedures;
- software licences and feature keys;
- site acceptance baselines;

- security certificates, accounts and remote-access paths; and
- knowledge held by the vendor’s support team rather than in operator documentation.

That inventory is part of the replacement scope. Without it, an Open RAN programme may appear to have an interoperability problem when it actually has a missing-data or missing-ownership problem.

Worked Example: One Vulnerability Across a 500-Site Open RAN

Consider an operator migrating 500 sites. It uses one O-RU supplier, a second supplier for O-DU and O-CU software, a commercial O-Cloud platform, a separate SMO, and three rApps from two developers. A prime integrator completed initial acceptance.

A severe vulnerability is then disclosed in a common software library. The library may appear in the SMO plug-in framework, an rApp container and a management agent packaged with the O-DU. This is where an Open RAN software supply-chain process either earns its keep or becomes paperwork.

1. **Find:** machine-readable SBOMs identify the exact builds containing the affected library. The asset inventory maps those builds to lab, pilot and production sites.
2. **Assess:** each supplier explains whether the vulnerable function is compiled, reachable and enabled. The operator verifies the claim against its own configuration and exposure.
3. **Contain:** access rules or feature controls reduce exposure while fixes are prepared. A containment change is tested for radio and management impact.
4. **Build trust:** suppliers deliver signed patches with provenance, release notes and updated SBOMs. The registry rejects unsigned or unexpected images.
5. **Integrate:** the operator tests the new SMO, rApp and O-DU combinations, including certificate use, alarms, performance and failover.
6. **Stage:** deployment moves from lab to a small field ring before the fleet. Automated health checks stop promotion when a defined threshold fails.
7. **Recover:** each layer has a tested rollback path. Restoring the old container is not enough if a database schema, certificate or configuration format changed.
8. **Close:** the operator records deployed versions, residual exposure, exceptions and supplier response times.

The SBOM accelerates discovery, but it does not decide exploitability, integrate the fix or assign liability. The prime integrator helps, but only if the support contract remains active after acceptance and includes third-party patch coordination. The operator remains responsible for deciding when production risk justifies deployment.

This example also reveals a hidden benefit. In a conventional stack, the same vulnerable library might exist but remain opaque until the integrated vendor investigates it. Open RAN can improve the evidence available to the buyer. It also removes the excuse that software provenance is entirely somebody else’s internal matter.

What to Require in an Open RAN RFP

Security requirements should enter the procurement before products and prices have fixed the architecture. NTIA’s full Open RAN security report recommends cradle-to-grave supply-chain management and explicitly calls for security requirements in RFPs and RFQs, supplier-process detail and SBOMs. A practical RFP should request evidence, not a promise to follow industry best practice.

RFP requirement	Minimum acceptable evidence	Reason
Product and software identity	Model, hardware revision, firmware or image digest, component owner and support status	Prevents evidence from being detached from the delivered build
SBOM delivery	Signed SPDX or CycloneDX file for each release, with update obligations	Supports component and vulnerability mapping
Secure development	Documented development controls, code review, build protection and vulnerability handling	Addresses how software is produced, not only how it is tested at the end
Package provenance	Signed artefact, protected signing process, trusted registry and verification instructions	Reduces substitution and pipeline tampering risk
Application permissions	Machine-readable permission and data-access manifest for each xApp or rApp	Limits the effect of a compromised or defective application
Interface security	Supported protocol profile, TLS version, certificate process and negative-test results	Open specifications still permit weak implementation or configuration
Vulnerability service	Notification channel, severity method, response target, mitigation process and historical record	Measures lifecycle performance after purchase
Remote access	Access architecture, approval flow, MFA, session logging and revocation	Identifies operational control outside the operator
End of life	Support dates, notice period, source or escrow options where appropriate, and migration assistance	Reduces the risk of an unsupported but irreplaceable component
Subsupplier change	Advance notification and buyer approval for defined material changes	Keeps initial due diligence valid during the contract

Evidence should be model-specific and version-specific. A corporate ISO certificate, penetration-test cover page or generic security brochure can support due diligence, but none proves how the delivered release was built or configured.

Test the System Between the Products

Open RAN failures often sit between individually conforming components. NTIA's own integration work describes multi-vendor interoperability as both the architecture's promise and its greatest challenge, with timing, compatibility and hardware dependencies requiring lab work. The same principle applies to security.

A useful acceptance and regression plan includes:

- mutual authentication and rejected-identity tests on every relevant interface;
- expired, revoked, malformed and untrusted certificate behaviour;
- least-privilege checks for operators, services, xApps and rApps;
- tampered, unsigned and downgraded software-package rejection;
- loss, delay and malformed-message tests across management and control interfaces;
- resource exhaustion and noisy-neighbour behaviour on the O-Cloud;
- RIC application conflict, removal and fallback behaviour;
- SMO outage, backup restoration and audit-log continuity;
- supplier remote-access enablement and emergency revocation;
- upgrade compatibility, partial-deployment failure and full rollback; and
- radio performance and service continuity after every security change.

Conformance testing asks whether an implementation follows a specification. Interoperability testing asks whether two implementations work together. Security testing asks whether they reject unsafe behaviour. Operational testing asks whether the operator can detect and recover from failure. A serious programme needs all four.

Do Not Leave the Integration Boundary Uncontracted

The old phrase "one throat to choke" is inelegant, but it describes a real procurement need: one party must own restoration while specialists investigate the root cause. In a multi-vendor RAN, this role can belong to the operator, a neutral system integrator or a prime contractor. It should never be left to goodwill during an outage.

Contracts should define:

- who leads a cross-vendor incident and who has authority to require diagnostic support;
- one severity scale and one incident clock across suppliers;

- how logs, packet captures, core dumps and sensitive configuration may be shared;
- who maintains the supported-version and compatibility matrix;
- which party runs regression tests after a component update;
- who pays when a required security patch breaks an adjacent product;
- how emergency changes are approved, recorded and reversed;
- what happens if a supplier is acquired, restricted, insolvent or ends support;
- the operator’s rights to audit evidence and use independent testing; and
- the continuing role of the integrator after rollout acceptance.

A service-level agreement for each box is not an end-to-end service agreement. The architecture needs a named owner for the gaps.

When Is Open RAN the Better Post-Huawei Choice?

Open RAN is most defensible where the operator wants supplier optionality and is willing to build the operating model that makes optionality real.

Open RAN is a stronger fit when…	Proceed cautiously when…
The operator has an integration lab and controlled production rings	The first meaningful integration test will occur at live sites
Architecture ownership, cloud ownership and security authority are explicit	Every supplier assumes another party owns the management and cloud boundary
At least two practical implementations have passed the required profile	Substitution exists only in a standards diagram
SBOMs, signed artefacts, asset mapping and vulnerability workflows are operational	SBOMs will be stored as procurement PDFs and never correlated with deployed versions
A prime integrator remains accountable through operations	Integration responsibility ends at commissioning
The business case includes testing, orchestration, skills and lifecycle support	The comparison uses radio-unit prices but omits integration and cloud operations
Security requirements are verified per release	Membership, certification or country of origin is treated as complete assurance

For a smaller operator without these capabilities, a managed Open RAN service or a prime-integrator model may be safer than assembling every layer directly. That reduces some commercial independence, but it does not defeat the purpose if interfaces, evidence and substitution rights remain available to the operator.

For a large operator, the strategic value may justify greater internal ownership. The organisation can use common labs, deployment pipelines and security operations across several vendors, then make replacement a rehearsed procedure rather than a promise in the architecture.

The decision should therefore be framed as an operating-model choice. Open RAN after Huawei can broaden the supplier market and make hidden dependencies more visible. It

can also produce a longer chain of software, identities and contracts. The architecture earns its security advantage only when the buyer can trace that chain from source and build evidence to a running workload, then restore service when one link fails.

Buyer rule of thumb: count control points, shared dependencies and unresolved ownership boundaries, not vendor logos. A five-vendor system with one opaque build pipeline is less diverse than it looks.

Ask for the incident map before approving the vendor map.

For one proposed Open RAN configuration, select a realistic event: a stolen signing key, a critical library vulnerability, an expired certificate or a failed O-Cloud upgrade. Ask the bidders to show who detects it, who decides, who patches, who tests, who rolls back and who restores service.

Can the proposed multi-vendor team answer that sequence with named people, evidence and time limits before the contract is signed?

Related procurement and engineering guides

White-Label Telecom Procurement Telecom Energy Standards 5G Site Power Trends

Contact Us

For catalog requests, pricing, or partnerships, please visit: https://www.thesolartelecom.com

Open RAN After Huawei: More Vendor Choice or More Software Supply-Chain Risk?