Stakeholders must collaborate to prove the security benefits of Open RAN and de-risk early deployments

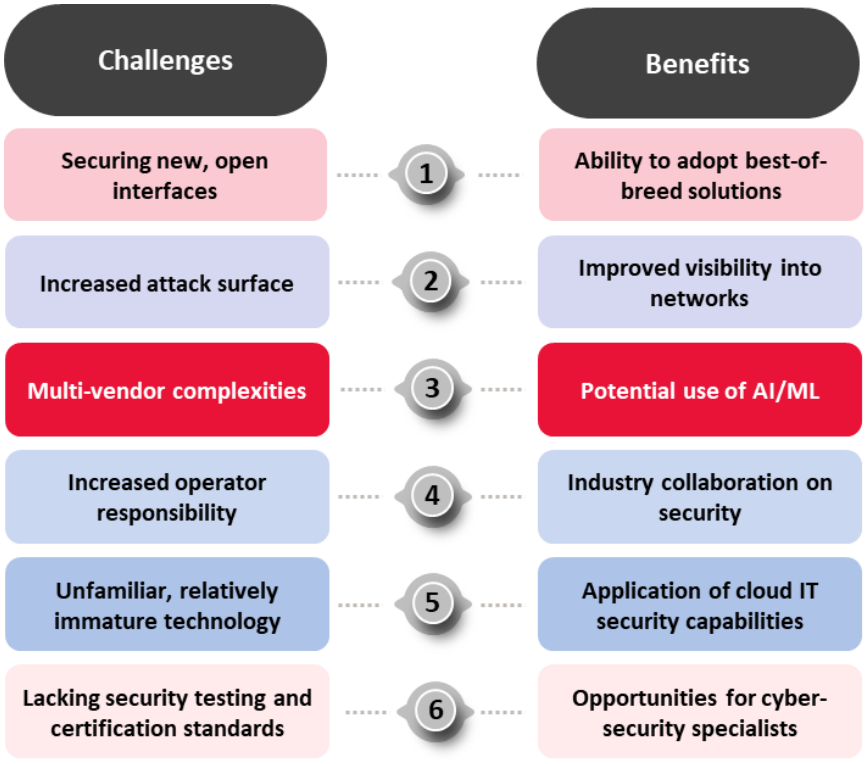
April 2025

James Kirby

The following article is a short summary based on Analysys Mason's report, *Considerations and strategies for cyber security*, which provides recommendations for vendors, operators and the ecosystem to help further de-risk Open RAN deployments.

There is a lack of consensus about whether Open RAN architectures will in aggregate be beneficial or detrimental to network security; however, operators commonly cite security and privacy issues as key challenges with Open RAN adoption. Stakeholders must de-risk initial Open RAN deployments by driving progress towards robust security certifications, implementing best practices ahead of standardisation, and by collaborating to prove the security benefits of a cloud-based, intelligent Open RAN.

Figure 1: Challenges and benefits of Open RAN to network security, 2025



Source: Analysys Mason

Open RAN introduces new security issues, with many believing it will make RAN security more challenging overall

An Analysys Mason survey of 67 Tier 1 and Tier 2 operators conducted in 4Q 2024 found that 34% of respondents thought that Open RAN will make it harder to address security challenges than traditional or closed

vRAN, while 33% said the reverse. Such contradicting opinions about Open RAN security are common. For example, some pundits claim that the increased number of open interfaces will pose a considerable security challenge while others argue that proprietary interfaces are not necessarily more secure and that the greater visibility into Open RAN architectures makes vulnerabilities and threats easier to spot. Given that security failings can lead to hefty fines and reputational damage for operators, this uncertainty is contributing to slowed Open RAN adoption.

Even if security does not necessarily become more challenging, the move to multi-vendor, cloud-based architectures will require operators to rework their security practices and vendors to change how they support operators with network security. For example, the move to multi-vendor architectures means that operators are less able to rely on a single vendor for RAN security.

In addition, O-RAN Alliance security standards are still immature in some areas, particularly in relation to testing and hardening requirements (especially relating to the Service management and orchestration (SMO) framework and the RAN intelligent controller (RIC)). Standards and testing specifications are important to ensure consistency in security between vendors and to reduce the risk of misconfigurations. They are also a requirement to support the development of recognised, industry-led certifications that can help de-risk Open RAN for operators, both in the context of network security, and their dealings with regulators.

Progress is needed to de-risk and reduce the burden of Open RAN security, particularly relating to multi-vendor deployments

Some operators have and will continue to move ahead with Open RAN deployment in the near term, despite the additional near-term security risks it poses. The security challenges with Open RAN can be effectively managed if operators and vendors (and systems integrators) take appropriate steps to secure networks ahead of standardisation, by adopting available best practices from the broader telecoms sector and IT industries and carrying out rigorous testing and audits. Operators can also de-risk their deployments by opting for a phased approach to multi-vendor adoption, adopting a single vendor first, followed by robust multi-vendor pre-integrations.

However, to drive progress towards widespread, at-scale commercial adoption of multi-vendor Open RAN (and support ecosystem diversity) it is imperative that progress is made to build confidence in its security and reduce its related operational burden. Critically, the industry must advance standardisation with a goal to reach recognised security certifications that can create consistency in the ecosystem and de-risk and reduce the burden of multi-vendor security for operators. Vendors and their partners must also leverage and prove the capabilities of a cloud-based, intelligent Open RAN to improve mobile network security posture (for example, using the SMO/RIC to improve anomaly detection, network resilience and to automate configuration testing).

Robust certifications and proof of Open RAN's security benefits will be critical in driving confidence and de-risking at-scale deployments

It is essential that vendors, operators and the Open RAN ecosystem drive progress to support consistency and confidence in Open RAN security. In our latest report on Open RAN security we discuss a range of recommendations for the industry in detail, based on three areas: multi-vendor networks, the AI-driven RIC/SMO, and open cloud deployments. These are summarised as follows:

- **The Open RAN ecosystem must drive progress towards robust security certifications** and use comprehensive testing frameworks and automated testing tools to simplify and de-risk Open RAN security.

Maturity in testing specifications will be critical to this progress, and stakeholders should also see automated testing vendors as key partners that can aid the security of E2E solutions, while reducing the burden of multi-vendor security tests.

- **Operators and vendors should trial SMO/RIC security features** that could support an optimal zero-trust architecture, partnering with security and testing specialists to drive progress and prove their value. The SMO, RIC and related artificial intelligence/machine learning (AI/ML) could provide substantial long-term benefits to Open RAN's security posture, however they are also the elements of Open RAN that face the highest number of risks and challenges for security. Operators, vendors and the wider industry should collaborate to drive progress in their standards.

- **Operators should de-risk their o-cloud deployments** by using the increased visibility, agility and automation brought by network softwarisation/virtualisation. Operators should aim to automate the security scanning and testing of their o-cloud and effectively use the telemetry data exposed by o-clouds, potentially with AI/ML-based threat detection and response tools, to harden o-cloud security.

For more information, please visit *Considerations and strategies for cyber security*.