WIND™

AN INTEL COMPANY

OPEN SOLUTIONS FOR NFV

A Checklist for Achieving the Benefits and Managing the Risks

"Openness" is one of the critical requirements for Network Functions Virtualization (NFV), a telecom initiative in which network functions are virtualized and run on commercial off-the-shelf (COTS) hardware. Open solutions significantly increase the number of software suppliers, which in turn increases the rate of innovation. By adopting an open strategy for their NFV architecture, telecom equipment manufacturers (TEMs) can develop new solutions faster, while lowering development costs. In addition, as network infrastructures transform to keep pace with the rapid increase in data traffic from new user behavior and new connections for the Internet of Things (IoT), employing a pragmatic open NFV strategy can facilitate improved capital and operational efficiencies, reducing total cost of ownership.

Fundamental to a successful open NFV strategy is adherence to the critical standards programs currently underway. The objective of these standards activities is to achieve plugin compatibility for NFV software components developed from a large ecosystem of independent software vendors (ISVs). But open standards face numerous challenges that, if not adequately addressed, could have a negative impact on the NFV market and impede deployment of NFV solutions. One key challenge is that standards typically evolve more slowly than the market, but vendors need to implement solutions today. This conundrum usually results in variations of implementations as vendors strive to comply with evolving standards while maintaining competitive differentiation and gaining time-to-market advantages.

The success of adopting an open NFV strategy depends greatly on the NFV software platform serving as the foundation. Today, available open NFV platforms range from bare-bones software platforms designed for a do-it-yourself approach, providing basic virtualization functionality, to fully integrated, ready-to-deploy, carrier grade compliant, virtual network function (VNF)–ready servers. The following seven questions will help you evaluate the suppliers of open NFV platforms and determine which approach best fits your product and business requirements.

QUESTIONS TO ASK SUPPLIERS

1. Does your NFV platform actively follow and implement critical open standards?

In providing an NFV platform, a supplier should be supportive of all NFV-related open standards, while actively trying to implement ahead of standards. Waiting for standards to be fully defined and ratified will usually mean being late to market. It is critical that platform suppliers actively participate in the critical working groups to ensure they have deep knowledge of the evolving standards and are implementing APIs and features that

are "future-proofed" to comply with the standards as they evolve. You should also look for vendors who participate and contribute in the areas that prioritize the specific needs of telecom, such as carrier grade and real-time APIs and features.

Wind River® participates in critical standards activities, including the following open standards forums: ETSI NFV and the Open Platform for NFV (OPNFV), OpenStack, the Yocto Project, Kernel-based Virtual Machine (KVM), and the Data Plane Development Kit. In particular, Wind River is active in working groups to help define and create HP APIs and real-time hypervisor capabilities.

2. Does your NFV platform implement vendor-neutral and standards-compliant APIs?

To achieve interoperability for NFV solutions, an NFV platform must employ an open architecture incorporating software that complies with all relevant API standards, including APIs for VNFs, for northbound NFV orchestrators and SDN controllers, and for operations support system/business support system (OSS/BSS) software. Implementing standards-compliant APIs ensures that NFV solutions will have the flexibility to use any API-compliant software components, and enables developers to add extensions or competitive differentiating features without causing interoperability problems.

Wind River Titanium Server, a fully integrated, VNF-ready NFV platform, is 100% compliant with all relevant API standards, such as ETSI MANO, OpenStack, and KVM. Wind River employs an open "plug-in" architecture for OpenStack that supports the interoperability of standard open source components and API-compliant custom software, and at the same time provides telecom-compliant OSS/BSS interfaces and operational, administrative, and management (OAM) features.

Does your NFV platform implement features and fixes ahead of the open source community to give you an early competitive advantage, or just provide "vanilla" open source? The speed of open source software development is slow compared to the speed of the NFV market. This is particularly true for ETSI-based management and orchestration (MANO) standards as well as for carrier grade capability for OpenStack. OpenStack, in particular, prioritizes enterprise applications over telecom, so carrier-required features can be delayed 12–24 months. By closely following the standards and open communities, yet incorporating carrier grade plugins and extensions into an NFV platform ahead of an open source contribution, TEMs and service providers can significantly benefit from an earlier market entry.

Wind River continues to incorporate carrier grade extensions to Carrier Grade Linux, KLM, OpenStack, and its middleware in advance of the rest of the industry. Wind River up-streams hardened versions for adoption by the rest of the open source community. For example, Wind River makes the source code available from its Accelerated vSwitch KLM and Poll Mode Drivers and up-streams enhancements to OpenStack and Carrier Grade Linux.

4. Does your NFV solution include differentiated non–open source software that can give you a competitive advantage without vendor lock-in?

It is often necessary to implement features such as carrier grade reliability in advance of the standards and open source community. As long as the platform provides open, published APIs between all levels of the ETSI architecture and OpenStack, vendor lock-in can be avoided. Openness is not an end in itself but a means to an end—there are instances when vendor-specific software will be superior to open source software, or provide some feature not available in open source software, giving communications service providers (CSPs) and TEMs a significant competitive advantage. However, it is critical that the platform supplier employ an open architecture and be committed to incorporating all necessary future functional equivalents of an open source version if one becomes available. As stated previously, Titanium Server employs an architecture that is compliant to ETSI, OPNFV, and relevant API standards.

For example, performance, scalability, and security requirements are more stringent for virtual switching in a carrier network. The Open vSwitch (OVS) currently has design limitations that result in inferior scalability and performance efficiency. To address these issues, Wind River has designed the Accelerated vSwitch (AVS) specifically for the NFV market. It employs performance optimizations and incorporates all the telecom-required functionality provided by OVS. Currently, AVS achieves line rate performance using fewer cores, without bypassing any controls such as QoS, rate limiting, security controls, live migration, or link protection. Because the vSwitch uses fewer cores, more cores become available for revenue-generating VNFs. AVS does not result in vendor lock-in, as the APIs and Neutron plugins to OpenStack provide the required abstraction.

5. Does your NFV platform require a carrier grade compliant open solution?

NFV is rooted in IT virtualization, but carrier requirements in many areas are more stringent than those for enterprise networks. Although virtualization and IT technologies are employed for NFV, carrier networks still need to maintain high levels of availability, performance, security, and scalability, and provide more sophisticated telecom-compliant management features.

Enhanced carrier grade capabilities have been incorporated into Titanium Server in areas such as fault tolerance, telecom alarms, diagnostics, operations management, traffic management, and security. Titanium Server achieves six-nines (99.9999%) infrastructure availability, in-service upgrades, hitless failover, live patching, efficient scalability, and low maintenance costs. Its optimized KVM and AVS provide deterministic, predictable performance using fewer computing resources than other commercial solutions. It also integrates telecom-compliant security features, including complete AAA access control.

But carrier grade is more than a set of features—the term also encompasses design techniques, practices, and tools that are used to harden the carrier grade features. Titanium Server is built on decades of carrier grade development expertise. It is designed to be compliant to TL9000, a key standard in the telecom industry, resulting in stable, predictable software releases and fast problem resolution.

6. Does your NFV platform solution require the time-to-market advantage of a fully integrated, ready-to-ship version?

Because NFV solutions are complex, the integration of multiple disparate open source software components onto a standard hardware platform can be an onerous task. It requires much more than just the testing of the software; dependencies must be identified and understood, and the different software components must be developed and integrated in such a manner as to make the platform operate reliably and with optimal performance. In-house integration often faces significantly more risk than a pre-integrated NFV platform due to unforeseen stability and interoperability problems, which can result in deployment delays and costly redesign. A pre-integrated platform achieves faster NFV product introduction times at lower development and support costs. Developing and integrating carrier grade extensions to the open source components provides a further benefit of delivering telecom-compliant NFV solutions earlier to market. Titanium Server is a fully integrated, VNF-ready carrier grade NFV infrastructure software platform that employs an open standard "plug-in" architecture that is compliant with ETSI NFV and OPNFV.

7. Does your NFV platform have an extensive ecosystem of hardware and VNF vendors?

Your NFV platform supplier's ecosystem can give you a significant competitive advantage by increasing your access to NFV technology and feature innovations without requiring the investment in internal resources. Wind River has established an extensive NFV ecosystem, Wind River Titanium Cloud, which is targeted at solutions and applications required by carriers. It consists of industry-leading hardware and software companies whose products have been pre-integrated and validated with Titanium Server. The Titanium Cloud ecosystem has been established to augment Wind River NFV technology to give customers the flexibility to build complete NFV solutions from the ecosystem. Furthermore, Wind River customer partnerships result in customer-driven requirements and features.

In summary, when evaluating a platform for your NFV solution, openness plays an important role—but it's not as simple as it may seem. There are factors that need to be considered alongside the open requirements. Use this checklist to ensure your solution will truly be open—for business.

WIND
AN INTEL COMPANY

Wind River is a world leader in embedded software for intelligent connected systems. The company has been pioneering computing inside embedded devices since 1981, and its technology is found in nearly 2 billion products. To learn more, visit Wind River at www.windriver.com.