

# WIND RIVER TITANIUM CLOUD FOR TELECOMMUNICATIONS

Carrier networks are undergoing their biggest transformation since the beginning of the Internet. The ability to get to market quickly and to respond to constantly changing network demands and location-based demographics is the key to success and growth. At the same time, video, mobile, and cloud usage is driving huge growth in traffic and overwhelming current networks.

To meet these challenges and thrive, you must find new ways to architect and build secure network infrastructures that can improve agility and reduce operating costs. One approach is to apply successful IT technologies, such as commercial off-the-shelf (COTS) hardware and mass virtualization and cloud deployment of applications. Technologies such as OpenStack and Kernel-based Virtual Machine (KVM) have emerged as de facto standards for cloud and virtualization. Combined with data plane acceleration technologies and virtual machine (VM) management services, they are defining a new class of network virtualization platform. Wind River® Titanium Cloud™ is the industry's highest-performing portfolio of network virtualization platforms.

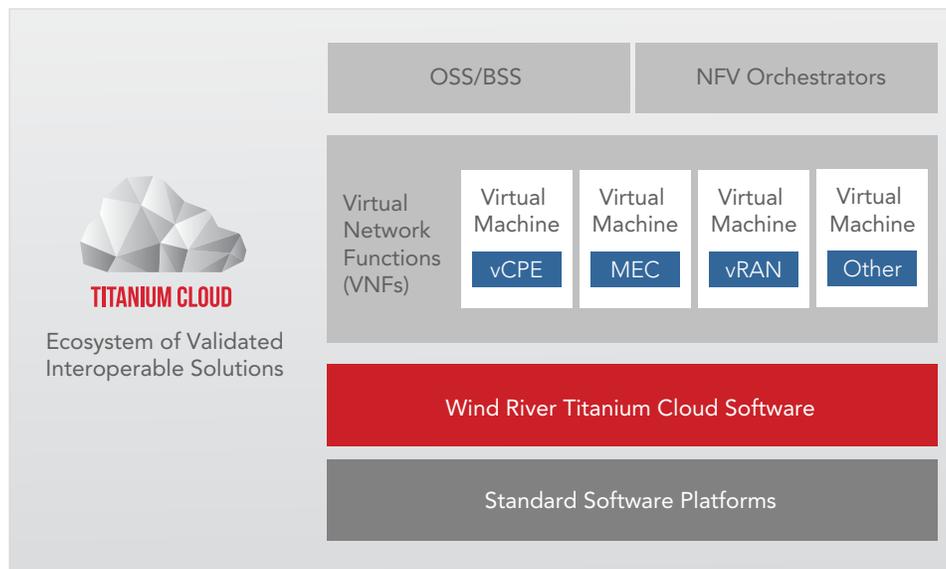
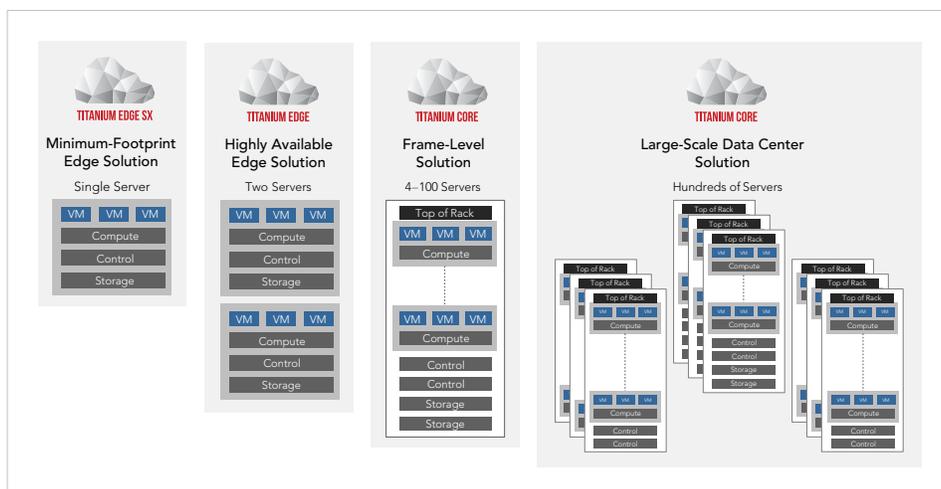


Figure 1: Complete end-to-end solution

## FULLY SCALABLE SYSTEM-LEVEL ARCHITECTURE

The Titanium Cloud portfolio of solutions for telecommunications (see Figure 1) includes Wind River Titanium Core, the industry's first fully integrated, highly optimized and carrier grade application-ready software solution; and Wind River Titanium Edge, the industry's smallest footprint for highly available network virtualization. The portfolio also includes Wind River Titanium Edge SX, a single-server configuration for minimum-footprint edge applications.

Titanium Core is the ideal platform to deploy critical services in data center environments that require real-time performance and continuous service availability. Titanium Edge provides the industry's smallest footprint for network virtualization and cloud solutions while maintaining full carrier grade reliability for services such as virtual customer premises equipment (CPE). Titanium Edge eliminates the need for additional controller hardware and combines workload applications, storage, and controller functions on two servers to deliver full carrier grade reliability and performance. Titanium Edge SX offers the telco-grade security, high-performance efficiency, and ultra-low latency needed for applications such as multi-access edge computing (MEC).



**Figure 2. Fully scalable system-level architecture**

The Titanium Cloud Ecosystem ensures a complete end-to-end set of solutions, including validated COTS platforms from leading hardware vendors and pre-validated virtual network applications. Wind River also provides all the support and professional services you need to develop and deliver complete solutions for network virtualization.

## BENEFITS OF USING TITANIUM CLOUD

- Accelerate your time-to-market by up to 18 months, removing the need to integrate, test, and document multiple technology components from different vendors and open source.
- Leverage 35 years of deep Wind River experience in deploying trusted, secure software systems to ensure the protection and ongoing integrity of your cloud infrastructure.
- Focus your development activities on revenue-generating applications.

- Reduce operating expenses by maximizing the performance and capacity of your virtualization platform.
- Lower your footprint and capital expenses for virtualized CPE and edge applications while maintaining high performance and high reliability where needed.
- Choose between running existing applications and management systems unchanged or optimizing for high performance and reliability.
- Maximize operational efficiency by giving your teams complete visibility into the network, with control where they need it and automation where they don't.
- Ensure compatibility and future proofing with APIs based on open source and de facto open standards.



Figure 3. The only commercial cloud platform that delivers true carrier grade reliability

## COMPONENTS

### De Facto Standard Open Source Software for Cloud and Virtualization

- **Linux:** Enterprise-focused Linux, plus 700+ patches, provides the reliability, security, availability, and performance needed for the carrier network.
- **Real-time KVM:** Based on years of embedded experience with KVM, Titanium Cloud adds kernel and user space optimizations to the industry-standard KVM hypervisor to deliver consistent and deterministic, predictable performance.
- **OpenStack:** OpenStack is the industry's leading open source cloud platform — but OpenStack is designed for IT-grade clouds. Titanium Cloud adds the reliability and availability extensions required to use OpenStack in the carrier network. This includes VM migration in hundreds of milliseconds rather than minutes, faster VM failure detection, automatic recovery of failed VMs, VM resource management, and faster host and controller node failover.
- **Ceph:** Ceph provides a highly scalable, highly available, highly performant distributed storage solution.

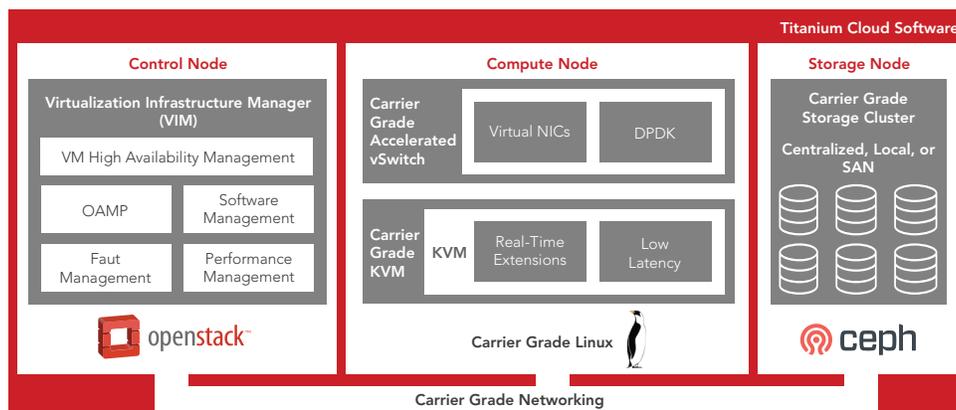


Figure 4. Titanium Cloud components

### High Performance and High Availability Where It's Needed

- **Accelerated vSwitch and inter-VM communication:** A high-performance user space vSwitch based on the Data Plane Development Kit (DPDK) enables high-performance VM-to-VM communication, bypassing the slow path through the Linux kernel, as well as high-performance packet processing from the network interface card (NIC) to applications in VMs. Support for DPDK, SR-IOV, and 1 Gb, 10 Gb, and 25 Gb Ethernet ensures ultra-fast packet processing.
- **Virtual infrastructure management:** Management tools designed for the carrier network are overlooked or non-existent in IT-based solutions. Titanium Cloud delivers live patching of platform components without loss of service, automation facilities for the application of patches throughout the cluster (saving significant manual labor), and hitless upgrade of platform software from one major release to the next for all nodes in the cloud.

### KEY FEATURES

#### Availability

- Fault tolerance to single and multiple software and hardware faults
- Hardware failover available with as few as two servers
- Support for a variety of redundancy models, including 1+1, N load-shared, N+1, and N+M, ensuring that a single fault cannot impact service
- Automatic VM recovery on failure of a host compute node (node failure detection in seconds rather than minutes)
- Automatic VM recovery on failure of a VM (60 times faster than standard IT grade)
- Fast live migration of VMs—even those using DPDK
- Controller node redundancy and automatic failover (not available in IT-based OpenStack)
- Optional high-resolution VM monitoring via guest VM-defined health checks
- VM protection groups (ensuring that VMs of the same group are created on different compute nodes)
- Minimal loss of service or data on failover

### Carrier Grade Management

- Overlay on top of OpenStack cloud VM management, providing six-nines availability
- Software management; live patching and hitless upgrade, including best-in-class orchestration facilities for measurable OpEx savings
- VM and application graceful shutdown
- VM management; fast and easy VM definition and creation
- High-availability management of applications
- Carrier grade fault management, isolation, and recovery
- Simplified telco deployment
- Platform and hardware alarms
- Extensive alarming with support for historical alarm queries
- Event logging for all non-alarm conditions
- Logs generated for all VM state transitions
- Seamless integration with telco OSS systems
- Pass-through application fault and performance feeds

### Carrier Grade Security

- UEFI secure boot and cryptographically signed images for host environment protection
- TLS with certificate storage in TPM hardware to protect management operations
- Industry-leading virtual TPM device (vTPM) that enables highest-security VM deployments
- Critical process monitoring and recovery on Titanium Cloud nodes for run-time environment protection
- Secure keyring database for storage of encrypted passwords
- Network firewall on external OAM interface for protection of management perimeter
- Role-based access control mechanism
- Secure password enforcement
- Active password aging
- Restricted access to root account and root commands
- Automatic logout of inactive user sessions
- External LDAP integration—keystone

### Performance and Scalability

- Predictable performance through validated and restricted resource assignment to VMs
- Automatic resource scaling, increasing or decreasing a VM's resources without requiring a restart
- Small two-node configuration ideal for CPE and appliance virtualization
- Single-node configuration ideal for MEC and small footprint use cases
- High scalability; hundreds of nodes, thousands of VMs, multiregions, including legacy infrastructure
- High-performance networking services delivered to VMs
- High-performance VM-to-VM communication
- Low latency interrupt and timer services to VMs

**REQUIREMENTS****Processors:** Intel® Xeon® class**NICs:** 1, 10, and 25 Gb DPDK-enabled ports supported**Operating system:** Minimum one core, recommended two cores**Virtual switching:** Minimum one core, recommended two cores**RAM:** Compute node minimum 32 GB; controller node minimum 64 GB**Disk:** Minimum 500 GB

Remaining cores and resources can be used for applications and virtual network functions.

**Networking Services**

- Guest network abstraction (logical versus physical)
- High-performance DPDK-based accelerated virtual switch for highest packet performance
- Support for SR-IOV and PCI pass-through
- Support for VM access to high-performance hardware encryption and compression accelerators
- Accelerated distributed virtual router (DVR); scalable accelerated routing with no single point of failure
- VLAN and VXLAN segment identification protocols
- Link aggregation group (LAG) for link redundancy and protection
- Private and public networking
- Intra-host and inter-host network connectivity
- Guest addressing and configuration (DHCP)
- Guest network isolation and security
- Integrated firewall
- Rate limiting
- Multi-segment and multi-tenant support
- Internet network connectivity
- Guest domain name services (DNSs)
- Network interface migration and associated addressing, state, and statistics

