SECURE VIRTUALIZATION PLATFORM FOR CRITICAL INFRASTRUCTURE

A Comprehensive Approach to Security with Titanium Cloud

INTRODUCTION

Companies, governments, institutions, and consumers are adopting cloud and cloud-based technologies at an ever-increasing rate, including (per a 2017 study by Schneider Electric[1]) those leveraging the cloud for security applications. This growing acceptance of the cloud as a reliable, valuable resource has an unfortunate and unintended consequence: The cloud has become a potentially lucrative target for those looking to hack, exfiltrate, or monetize via malware the data within the cloud.

True protection from attacks cannot be easily achieved; there are no quick software add-ons, no "all-in-one" security tools to deploy that fit the need. True protection must be comprehensive in approach, designed into the solution from the day the first line of code is authored through to a product's retirement. Protection must include technologies that safeguard against configuration flaws and problematic development practices, and technologies that detect subtle load tampering and prevent the theft of vital secrets. In short, the cloud must be made safe from the moment it boots and begins to provide service, continuing on through daily 24x7 operations.

Security is definitely not an afterthought for the award-winning Wind River® Titanium Cloud™ virtualization platform. Designed for hosting critical infrastructure applications (e.g., those involved in power generation, oil and gas refineries, chemical factories, and telecommunications systems), Titanium Cloud provides broad and deep protection from today's persistent industry threats and ever-present and evolving active attacks.

LIFECYCLE EVENTS

As part of a typical software product lifecycle, systems are architected, developed, and then deployed into the field. They power up, boot, and provide service; they are managed and receive updates. During each stage of this product lifecycle at Wind River, actions and specific formal procedures are followed to ensure the security and integrity of the Titanium Cloud family of products and the services they provide to applications.

Titanium Cloud Security Lifecycle Events

While not an exhaustive list, the following details provide some insight into the practices and technologies employed by Wind River in securing Titanium Cloud.

- During the development phase, engineers implementing Titanium Cloud features follow a rigorous development methodology that includes mandatory code inspections, update traceability, and architectural oversight.
- Prior to product release, a third-party security tool is used to actively probe each new Titanium Cloud runtime for vulnerabilities, misconfigurations, and potential attack vectors. Any findings are analyzed and evaluated, with written responses generated and actions taken.
- After all known issues have been addressed and the final build created, portions of the Titanium Cloud product load (boot loaders, the OS kernel itself, and supporting kernel modules) are cryptographically signed at Wind River to protect against any form of change or tampering while in transit to a customer site or after delivery.
- During the boot process in the field, low level system firmware ensures that crucial portions of the load being executed are bit-for-bit identical to that shipped by Wind River, as validated using cryptographic public key signatures (specifically, following a process known as UEFI Secure Boot and X.509 signatures).

- During onsite installation, customers' transport layer security (TLS) certificates, used to safeguard system management sessions, are securely stored in the hardware platform's Trusted Platform Module (TPM). This ensures that these private TLS keys are completely protected against all forms of exfiltration or tampering by the underlying hardware itself.
- Virtual machines hosted on Titanium Cloud, which require the highest levels of security, are launched by the system and assigned their own virtual TPMs. This ensures that these VMs are able to compartmentalize and securely protect their own key data, independent of the underlying platform. Thanks to innovations and R&D by Wind River, this same data can be securely migrated from one host to another during VM live migration, further enhancing the value of the feature.
- At runtime, embedded network filters, access control lists (ACLs), firewalls, and quality of service (QoS) policy control mechanisms are activated, protecting the platform and applications from both external and internal network threats.
- On a continuous basis, Wind River actively monitors industry security forums (e.g., US-CERT), reviewing and analyzing all new and potential critical vulnerabilities reported that may impact Wind River products, including Titanium Cloud. When necessary, software patches are developed to address discovered vulnerabilities, and our customers are informed to take action.

Titanium Cloud includes a best-in-class hitless patching system and patching orchestration engine, which together eliminate the need for service outages and significantly reduce the OpEx cost of software patch application over competing manual systems. These combined features eliminate the common barriers and delays that impede the proactive application of security updates.

For more than 30 years, Wind River has helped the world's technology leaders power generation after generation of the safest, most secure devices in the world. Companies managing or delivering critical infrastructure services can turn to the Wind River Titanium Cloud family of products to secure their cloud environments and safeguard their ongoing business operations.

To learn more about the Titanium Cloud family of products, please refer to www.windriver.com/products/titanium-cloud or contact us to arrange a face-to-face discussion.

1. Download Schneider Electric's survey report, "Security in the Cloud," at go.schneider-electric.com/NAM_PB_Buildings_US_201703_Security-Survey-Results-Web-01-Security-Survey-Results-MF-LP.htm.

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.