GalacticQSL Lightpaper

Zero-Trust Software Deployment for Space, Defence, and Edge Systems

Document Version: 1.0
Date: 10th March 2026
Classification: Public
Next Review: N/A

About This Lightpaper

This document is a lightpaper — a concise, accessible overview of a technology, product, or concept designed to give readers a clear top-level understanding without delving into deep technical implementation detail.

Lightpapers are intended for a broad audience, including technical and non-technical stakeholders, prospective partners, investors, and decision-makers who need to understand the strategic purpose, capabilities, and relevance of a solution. They sit between a marketing one-pager and a full technical white paper: substantive enough to convey real value, accessible enough to be read without specialist expertise.

For clients and partners requiring deeper technical documentation — including integration guides, runtime specifications, attestation protocols, and compliance frameworks — Pan Galactic provides dedicated technical materials upon request and under appropriate confidentiality agreements.

Executive Summary

Modern software systems increasingly rely on containerisation to package and deploy applications consistently across different environments.

Platforms such as Docker and Kubernetes have transformed how applications are delivered, enabling faster development and deployment cycles.

However, container technologies were primarily designed for commercial cloud environments. They were not originally built for:

- space systems
- defence infrastructure
- mission-critical edge computing

Galactic Secure Containers provide a hardened container framework designed specifically for these environments, integrating **post-quantum cryptography, secure attestation, and supply chain verification**.

The Problem

Software supply chain attacks have become one of the most significant cybersecurity threats facing modern organisations.

Attackers increasingly target:

- software repositories
- build pipelines
- deployment infrastructure

This creates risks where compromised software can be deployed without detection.

In mission-critical environments such as satellites, defence platforms, and autonomous systems, this risk is unacceptable.

Operators must be able to verify:

- that software has not been tampered with
- that approved versions are running
- that mission configurations are correct

Traditional container systems provide limited guarantees in these areas.

The Pan Galactic Solution

Galactic Secure Containers introduce a **zero-trust container infrastructure** designed for critical systems.

The system builds upon existing container standards while adding additional layers of security and verification.

Developers can continue using familiar container tooling while benefiting from stronger security guarantees.

How the Technology Works

Galactic Secure Containers remain compatible with the **Open Container Initiative (OCI)** ecosystem.

This allows developers to use common tools such as:

- Docker
- Podman
- Buildah

Containers are built using standard OCI formats, but execution occurs through a hardened runtime layer called the **Galactic Secure Runtime (GSR)**.

Architecture Overview

Developer Tooling
(Docker / Podman / Buildah)

↓

OCI Image Format

↓

Galactic Secure Runtime (GSR)

↓

GalacticOS Kernel Security Layer

This architecture preserves compatibility with existing developer workflows while enforcing stronger runtime security policies.

Secure Boot and Attestation

Galactic Secure Containers incorporate a secure execution chain beginning at hardware level.

The system can integrate with:

- Trusted Platform Modules (TPM)
- Hardware security modules
- secure enclaves

The container launch process follows a verified chain:

- Hardware root of trust verifies the boot chain
- GalacticOS kernel verifies the runtime environment
- Container image signatures are verified
- Runtime policies are validated
- Attestation proofs are generated

Verification records can be referenced through **GalacticQB**, creating a tamper-resistant audit trail.

Deployment Environments

Galactic Secure Containers are designed to operate across three classes of deployment environments.

Orbital compute systems

- Satellite onboard computers
- Radiation-hardened hardware
- Limited memory and intermittent connectivity

Containers in these environments must be lightweight, deterministic, and efficient.

Ground station infrastructure

- Mission operations software
- Telemetry pipelines
- AI-based data processing systems

Tactical edge platforms

- Mobile defence compute units
- Remote sensors
- Maritime systems
- Autonomous drones

These systems benefit from secure container deployment with offline verification capabilities.

Secure Container Registry and Marketplace

Galactic Secure Containers are intended to integrate with the **Galactic Sandbox**, a secure application registry.

This environment will allow approved developers to publish secure container images that can be deployed across the Pan Galactic ecosystem.

Capabilities include:

- secure container registry
- post-quantum code signing
- security audit pipelines
- mission-specific application certification
- access-controlled deployments

This creates a controlled ecosystem for software used in space and defence environments.

Blockchain Integration

The GalacticQB blockchain will be used to record verifiable metadata related to container images.

Rather than storing container images directly, the blockchain records information such as:

- image hashes
- developer identities
- version histories
- deployment events
- attestation proofs

This creates a tamper-resistant audit trail for the software supply chain.

Why It Matters

Galactic Secure Containers provide a secure software deployment mechanism designed for environments where trust cannot be assumed.

By combining:

- post-quantum cryptography
- secure runtime enforcement
- attestation verification
- blockchain provenance

Pan Galactic is building a container infrastructure capable of supporting mission-critical software systems.

How It Fits Into the Pan Galactic Ecosystem

Galactic Secure Containers act as the **onboarding layer for the Pan Galactic platform**.

Developers begin by deploying containerised applications.

Once applications are running within the ecosystem, they can integrate with:

- GalacticQS for quantum-safe cryptography
- GalacticOS for secure system infrastructure
- GalacticQB for trusted data and software provenance

This creates a secure foundation for software operating across space, defence, and edge computing environments.

Contact

For guidance on this document:
flow@pangalactic.io