GalacticOS Lightpaper

A Secure Operating System for Space, Defence and Critical Infrastructure

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 space and defence systems increasingly depend on software-defined infrastructure. Satellites, ground stations, communications networks and edge compute systems now run complex software stacks that manage mission operations, data processing and secure communications.

However, many of the operating systems used in these environments were designed decades ago. They were built before the emergence of modern cyber threats, before the rise of large-scale software supply chain attacks, and before the looming impact of quantum computing on cryptographic security.

GalacticOS is Pan Galactic's secure operating system designed for these new realities. Built on a hardened Linux foundation, GalacticOS integrates post-quantum cryptography, secure container infrastructure and cryptographic identity systems directly into the operating environment.

The result is a platform designed to support secure software execution, verifiable system integrity and quantum-resilient communications across space systems, defence infrastructure and edge computing environments.

The Problem

Operating systems form the foundation of every digital system. They manage hardware resources, enforce security policies and provide the environment in which applications run.

In critical infrastructure environments, the operating system must guarantee three things:

1. System integrity
2. Secure communications
3. Verifiable software execution

Many existing operating systems used in aerospace and defence were not designed with modern cybersecurity threats in mind.

Challenges include:

- Legacy cryptographic standards that may become vulnerable to quantum attacks
- Limited protection against software supply chain compromise
- Difficulty verifying that the correct software is running on mission systems
- Complex integration between security layers, containers and applications

In space systems these challenges are amplified by the constraints of orbital hardware:

- limited memory
- limited storage
- intermittent communications
- high reliability requirements

Operators need operating systems that can support modern security architectures while remaining efficient and reliable in constrained environments.

The Pan Galactic Solution

GalacticOS is a secure, modular operating system designed specifically for mission-critical environments.

It builds upon the stability and ecosystem of Linux while integrating additional layers of security, cryptography and system verification.

The operating system integrates several key technologies:

- Post-quantum cryptography through the GalacticQSL library
- Secure container infrastructure through Galactic Secure Containers
- Cryptographic identity and provenance through GalacticQB

Rather than relying on external security tooling, GalacticOS embeds these capabilities directly within the system architecture.

This allows operators to deploy software systems that are secure by design rather than relying on layered security patches.

How the Technology Works

GalacticOS combines several security layers to create a trusted execution environment.

Hardened Linux Foundation

GalacticOS is built upon a customised Linux distribution designed for reliability and modular deployment.

This approach provides several advantages:

- mature and widely supported kernel architecture
- compatibility with existing software ecosystems
- flexibility for embedded and edge environments

The system is hardened through security configuration, minimal system components and strict runtime policies.

Integrated Post-Quantum Cryptography

GalacticOS integrates the GalacticQSL cryptographic library directly into the operating system.

This enables applications and services to access quantum-safe cryptographic functions without requiring separate integrations.

Supported cryptographic capabilities include:

- classical cryptography such as RSA, ECC and AES
- post-quantum key exchange using Kyber (ML-KEM)
- post-quantum digital signatures such as Dilithium and SPHINCS+

This architecture allows organisations to maintain compatibility with existing cryptographic standards while preparing for post-quantum migration.

Secure Container Infrastructure

Applications running on GalacticOS are typically deployed through Galactic Secure Containers.

Containers allow applications to be packaged and deployed consistently across different systems while maintaining isolation between workloads.

GalacticOS integrates directly with the Galactic Secure Runtime, enabling the operating system to enforce strict security policies during container execution.

This approach provides several advantages:

- consistent software deployment across orbital and ground infrastructure
- strong isolation between mission applications
- cryptographically verified software execution

System Attestation and Provenance

GalacticOS can support secure boot chains and runtime attestation, allowing operators to verify the integrity of the system.

The verification chain may include:

- hardware root of trust
- secure boot validation
- kernel verification
- runtime policy enforcement

Verification events can be recorded through GalacticQB, providing a tamper-resistant record of system state and software execution.

For operators of critical infrastructure, this allows them to confirm:

1. that authorised software is running
2. that systems have not been tampered with
3. that mission configurations are correct

Standards and Compliance Alignment

GalacticOS is designed to support compliance with security standards used across space, defence and critical infrastructure sectors.

Relevant frameworks include:

- NIST cybersecurity standards
- ISO information security frameworks
- UK National Cyber Security Centre guidance
- ECSS space system security standards
- ETSI telecommunications standards
- 3GPP security frameworks

The system architecture is designed to support the growing requirement for crypto-agility, allowing organisations to transition cryptographic algorithms as standards evolve.

Deployment Environments and Use Cases

GalacticOS is designed to operate across multiple deployment environments.

Space Systems

- Satellite onboard computers
- Orbital compute platforms
- Autonomous mission systems

The operating system can support lightweight deployments suitable for constrained hardware environments.

Ground Infrastructure

- Ground station control systems
- Mission operations platforms
- Satellite telemetry processing

In these environments GalacticOS can support containerised workloads and data processing systems.

Tactical Edge Platforms

- Defence mobile compute systems
- Remote sensors
- Maritime and airborne systems
- Autonomous vehicles and drones

These environments benefit from the system's secure container architecture and cryptographic identity framework.

Why It Matters

As space and defence infrastructure becomes increasingly software-driven, the operating system becomes the central point of trust.

If the operating system cannot guarantee system integrity and secure communications, every application running on top of it becomes vulnerable.

GalacticOS is designed to address these challenges by embedding security directly into the platform architecture.

By integrating quantum-safe cryptography, secure container infrastructure and verifiable system attestation, GalacticOS provides a foundation for building resilient software systems in mission-critical environments.

How It Fits Into the Pan Galactic Ecosystem

GalacticOS acts as the core platform layer within the Pan Galactic technology stack.

It connects and enables the other major components of the ecosystem.

GalacticQSL provides cryptographic primitives used by the operating system and applications.

Galactic Secure Containers provide a secure method for packaging and deploying applications.

GalacticQB provides a trust layer for software provenance, system attestation and verifiable infrastructure.

Together these technologies form a unified platform designed to support secure software systems operating across space, defence and edge computing environments.

Contact

For guidance on this document:
flow@pangalactic.io