Post-Deployment Vulnerability Defense for Space Combat Power

Using Digital Twin Technology to Sustain Mission-Critical Software in Contested Environments

Author: Tracy Ragan, CEO, DeployHub

Intended Audience: Space Combat Power PEO Leadership, Program Managers, Chief Engineers, Cyber Resilience Leads, Platform Engineering and DevSecOps Architects

---

Executive Summary

Space combat power is increasingly defined by software. Mission applications, autonomy services, ground systems, and tactical cloud platforms are continuously updated and deployed across satellites, ground stations, and distributed edge environments. While the Department of Defense has invested heavily in shifting security earlier in the software lifecycle through static analysis, software composition analysis, container scanning, and pipeline gating, critical and high-risk vulnerabilities continue to appear in operational systems.

The scale of the problem is accelerating. Independent analyses of the National Vulnerability Database indicate that approximately **48,185 Common Vulnerabilities and Exposures (CVEs) were published in 2025 alone**. Of these, roughly **3,984 were classified as Critical severity** (CVSS ≥ 9.0) and **15,003 as High severity** (CVSS 7.0–8.9). In other words, **more than 18,900 vulnerabilities, about 39% of all reported CVEs in 2025, represent high or critical risk**. The majority of these vulnerabilities are disclosed **after software has already been fielded**, meaning operational systems inevitably inherit risk that could not have been prevented by build-time controls.

The root cause is not insufficient tooling, but a structural mismatch between build-time security models and the dynamic nature of operational software. Once software is deployed, it does not remain static. New vulnerabilities are disclosed daily, indirect dependencies evolve without code changes, and runtime environments continuously change through scaling, redeployment, and configuration drift. Pre-deployment security

establishes an initial baseline, but it cannot determine whether systems remain secure over time.

DeployHub addresses this gap with a post-deployment vulnerability defense model built on Digital Twin technology. By continuously modeling what is actually running in operational environments and correlating that state with vulnerability and compliance intelligence, DeployHub enables Space Combat Power programs to detect newly disclosed vulnerabilities affecting live mission systems, maintain continuous alignment with NIST Secure Software Development Framework (SSDF) and OpenSSF Scorecard practices, and automate remediation workflows that dramatically reduce mean time to remediate. This approach transforms security from periodic assessment into a persistent operational capability aligned with zero-trust and cyber-resilient system design.

The Operational Limits of Build-Time Security

Traditional DevSecOps pipelines are designed around the assumption that most risk is introduced before release. In operational space systems, this assumption no longer holds. Exploitable vulnerabilities are discovered after software is already fielded. A component that passed every pipeline check may become critically vulnerable weeks later when a new CVE is published. At the same time, modern mission software relies heavily on deep dependency graphs, where changes in transitive components can introduce risk without any modification to application code.

Runtime environments further complicate the picture. Containers and clusters are frequently re-provisioned as part of normal operations, changing the actual software composition of deployed systems. Programs therefore retain strong visibility into what they intended to deploy, but limited visibility into what is actually running at any given moment. This visibility gap allows risk to accumulate silently in operational environments, eroding cyber resilience and increasing mission exposure.

Post-deployment vulnerability defense focuses on closing this gap. Rather than relying solely on historical scan results, DeployHub continuously identifies the open-source components present in deployed workloads and correlates that information with real-time vulnerability intelligence. When a new vulnerability is disclosed, teams can immediately determine whether it affects operational systems, which applications are exposed, and who owns remediation. Response shifts from broad, reactive triage to targeted, mission-informed action.

Digital Twins for Mission Software

A Digital Twin is a continuously updated virtual representation of a real system. In DeployHub, the Digital Twin models mission applications, containers, open-source packages and versions, deployment environments, and lineage relationships between source, build artifacts, and runtime. This model is constructed by federating metadata from CI/CD pipelines, source code repositories, artifact registries, and Kubernetes audit logs.

Critically, this approach requires no endpoint agents, sidecars, or repeated rescanning of images and binaries. By eliminating runtime instrumentation and continuous rescanning, DeployHub avoids adding software footprint to mission systems, avoids performance overhead, and reduces infrastructure and sustainment cost. Instead of treating software bills of materials as static build artifacts, DeployHub maintains living SBOMs that evolve alongside operational systems. Every deployment change is reflected in the Digital Twin, providing near real-time visibility into actual software composition.

The Digital Twin becomes the authoritative operational model of mission software. It provides the foundation for correlating vulnerabilities, compliance signals, and ownership information with live workloads, enabling security to function as continuous operational control rather than periodic inspection.

Continuous Compliance in Operational Environments

Many compliance frameworks implicitly assume continuous monitoring, yet most tooling evaluates compliance only at discrete pipeline stages. DeployHub extends compliance into runtime operations by associating security posture and best-practice signals with the components that are actually deployed.

OpenSSF Scorecard is an open-source solution from the Open Source Security Foundation (OpenSSF.org) that grades open-source package compliance levels. DeployHub ingest scorecard results linked to deployed open-source components, allowing programs to determine whether mission-critical systems depend on projects with weak security practices and to prioritize mitigation accordingly.

Similarly, the NIST Secure Software Development Framework requires organizations to identify vulnerable components, monitor deployed software, remediate vulnerabilities, and maintain evidence. DeployHub directly supports these objectives by maintaining a live inventory of deployed components, continuously detecting newly disclosed

vulnerabilities, tracking remediation actions, and automatically generating audit-ready evidence.

Compliance thus shifts from a documentation exercise to an always-on operational state that evolves with the system.

From Detection to Automated Remediation

Visibility alone does not reduce risk. DeployHub closes the loop by tightly integrating detection with remediation workflows. When a critical vulnerability is identified in a running system, the Digital Twin determines which repository and dependency file introduced the vulnerable component. An AI-assisted engine proposes a safe version update and automatically generates a pull request. Existing CI/CD pipelines then validate and deploy the fix using standard processes.

This approach transforms vulnerability response from a manual, ticket-driven process into an automated pipeline. Programs typically observe reductions in mean time to remediate from months to days, improving cyber resilience while minimizing operational disruption.

Architectural Overview

DeployHub integrates with existing development, delivery, and runtime platforms to collect deployment metadata, build the Digital Twin, correlate vulnerability and compliance intelligence, and drive automation. It is currently at TRL 7. The architecture is designed to augment, not replace, current tooling investments.

As shown in *Diagram 1*, Data is collected from three primary control points: Git organizations, binary repositories, and Kubernetes audit logs. Together, these sources form the authoritative basis of the Digital Twin for every release deployed to an endpoint, on-orbit, cloud-native or edge.

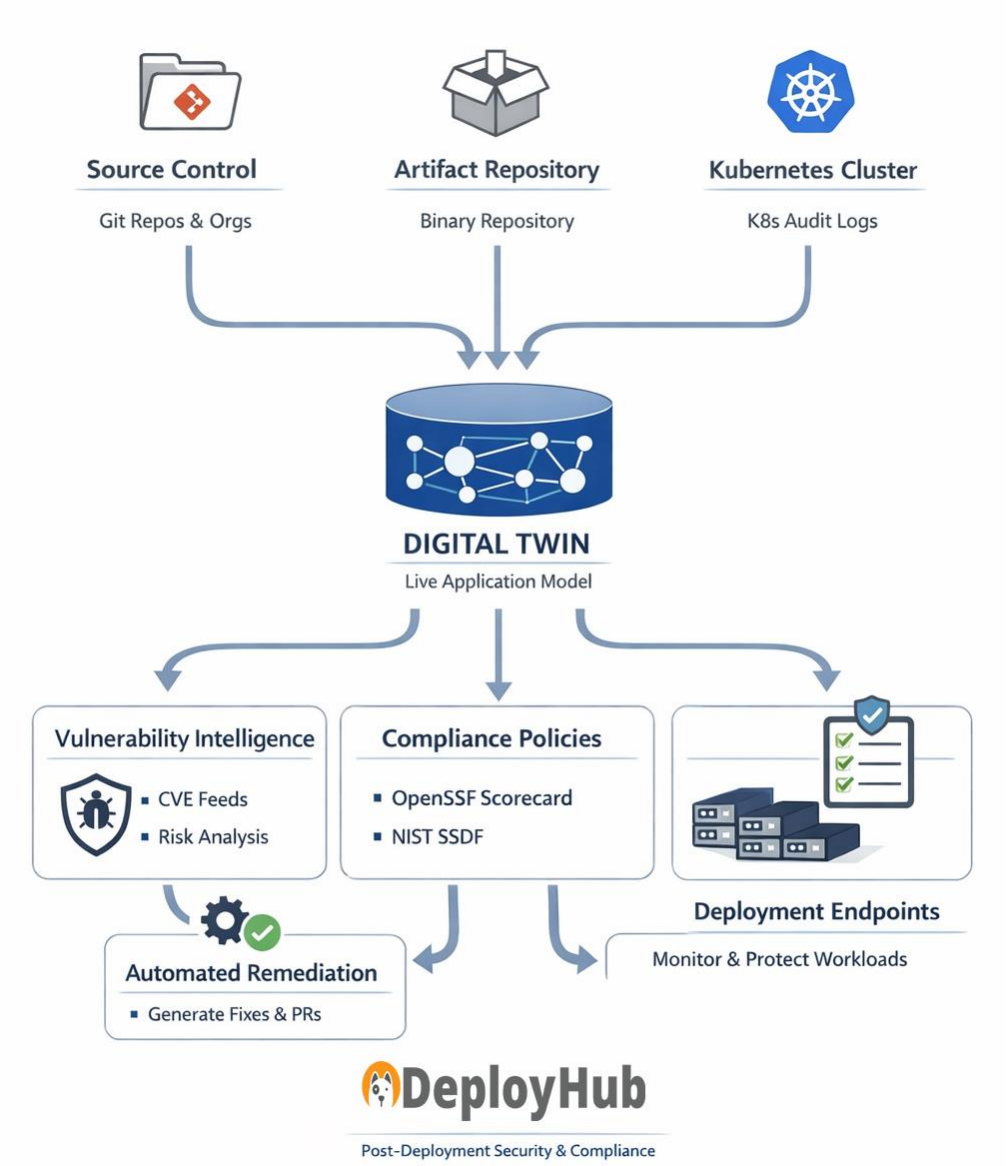
Source Control
Git Repos & Orgs
Artifact Repository
Binary Repository
Kubernetes Cluster
K8s Audit Logs
DIGITAL TWIN
Live Application Model
Vulnerability Intelligence
CVE Feeds
Risk Analysis
Compliance Policies
OpenSSF Scorecard
NIST SSDF
Deployment Endpoints
Monitor & Protect Workloads
Automated Remediation
Generate Fixes & PRs
DeployHub
Post-Deployment Security & Compliance

Diagram 1

Conclusion

Pre-deployment security answers whether software was safe when it was built. Post-deployment vulnerability defense answers whether it is safe while executing the mission.

By combining Digital Twin technology with continuous vulnerability detection, compliance correlation, and automated remediation, DeployHub enables Space Combat Power programs to sustain cyber-resilient, mission-ready software in contested environments. Security becomes an operational capability, always on, continuously validated, and tightly coupled to mission execution.

Contact Information

Tracy Ragan, CEO
Tracy@DeployHub.com

Website:
DeployHub.com

Government Info:
DeployHub.com/government-open-source-security/

UEI: D2NDAMGPJZ69
Cage Code: 03N22

HQ
30 N Gould St Ste 36977 Sheridan
WY 82801-6317 US