leidos

UpHold Aware™

CNAPP for Multicloud Federal Missions

Operationalizing Cloud Security for Federal Missions

Table of Contents **Page**

Executive Summary

Federal agencies are accelerating modernization through cloud and cloud-native platforms to deliver mission capabilities with greater speed and resilience. Most programs now operate across multicloud and hybrid environments, increasing flexibility – but also expanding complexity and attack surface.

Leidos delivers UpHold Aware™, a mission-integrated cloud-native application protection platform (CNAPP) capability designed to help federal agencies secure multicloud and hybrid environments at scale. The solution incorporates leading cloud-native technologies, including Wiz, to provide unified visibility, risk correlation and accelerated remediation.

By combining Leidos' deep federal mission expertise with Wiz's agentless, graph-based CNAPP platform, organizations stand to gain:

- A consistent security model across multicloud environments
- Prioritized risk insights aligned to mission impact
- Faster, more efficient remediation at scale

This partnership helps federal programs move beyond fragmented tooling toward integrated, outcome-driven cloud security.

The federal cloud challenge:

Cloud-native modernization changes the nature of cybersecurity work. Systems evolve daily through infrastructure-as-code (IaC), CI/CD pipelines, container image updates, managed services adoption and elastic scaling. The "assets" to secure are no longer only static servers; they are dynamic services, identities, APIs, containers and configurations that can shift continuously.

Federal programs must continuously answer critical questions:

- Are cloud environments configured securely and consistently?
- Which risks are truly exploitable and mission-relevant?
- How do identity and access decisions impact overall risk?
- Are we preventing issues early or reacting too late?

The UpHold Aware approach to CNAPP

Leidos delivers UpHold Aware's CNAPP as a mission-integrated capability designed specifically for federal multicloud and hybrid environments. The architecture

incorporates cloud-native technologies, including Wiz, to unify visibility across cloud posture, workloads, identities and development pipelines.

Rather than treating CNAPP as a toolset, UpHold Aware applies cloud-native telemetry to:

- Align security findings to mission systems and priorities
- Integrate zero trust architectures
- Support federal compliance frameworks (NIST, FedRAMP)
- Support actionable, program-level decision making

Within UpHold Aware's CNAPP, "mission-aware" security refers to the ability to correlate technical cloud risks with operational mission impact, system criticality, data sensitivity and federal risk priorities. This helps organizations focus remediation efforts on the issues most likely to affect mission delivery, operational resilience and zero trust objectives.

Core UpHold Aware CNAPP Capabilities

1. Unified security posture across multicloud and Kubernetes

Leidos delivers unified multicloud security posture management through an integrated CNAPP capability that is designed to provide visibility across AWS, Azure, GCP, OCI and Kubernetes environments. The capability leverages agentless cloud-native technologies, including Wiz, to accelerate deployment and reduce operational overhead.

Leidos enhances this by:

- Defining baseline configurations aligned to federal standards
- Mapping posture findings to mission systems, enclaves and hybrid Kubernetes environments (including on-prem clusters where applicable) to provide more complete defensive cyber picture
- Supporting continuous compliance and audit readiness

Intended outcome:
Consistent, scalable posture management across complex federal environments designed to decrease operational burden.

2. Cloud workload protection platform (CWPP) and risk-based vulnerability management

Leidos delivers risk-informed workload protection and vulnerability management designed to help federal programs prioritize exploitable risks across multicloud environments. The capability incorporates graph-based cloud analytics and agentless visibility technologies, including Wiz, to correlate vulnerabilities, exposure paths and runtime context.

Leidos operationalizes this by:

- Prioritizing vulnerabilities based on mission impact and exploitability
- Integrating findings into existing SOC and DevSecOps workflows
- Driving remediation through clear ownership and accountability

Intended outcome:
Reduced noise and faster remediation that is focused on what actually threatens mission operations.

3. Identity and entitlement risk management

Leidos supports identity-aware cloud risk management aligned to zero trust principles across multicloud and hybrid environments. Integrated analytics capabilities help identify excessive permissions, risk access relationships and lateral movement paths across workloads and cloud services.

Leidos extends this capability by:

- Aligning identity risk with zero trust principles
- Supporting least privilege implementation at scale
- Identifying cross-workload and multicloud risks

Intended outcome:

Improved control over “who can do what,” helping reduce lateral movement risk across mission systems

4. Shift-left security and supply chain assurance

UpHold Aware extends cloud security visibility into development pipelines to help identify infrastructure-as-code and container risks before deployment. The capability incorporates cloud-native analytics technologies, including Wiz, to support early-stage risk identification and remediation.

Leidos enables this by

- Integrating risk-informed security checks into development workflows, helping developers prioritize and remediate vulnerabilities based on real-world exposure and potential mission impact

- Supporting federal supply chain risk management requirements
- Aligning early-stage findings with runtime risk context

Intended outcome:
Reduced rework, improved software assurance and stronger alignment with secure-by-design principles.

Operationalizing mission-aware CNAPP for federal missions

UpHold Aware CNAPP combines cloud-native security telemetry, operational context and federal cyber expertise to help agencies prioritize and remediate the risks most relevant to mission execution The capability integrates graph-based cloud analytics technologies, including Wiz, within a broader operational framework aligned to federal architectures, zero trust initiatives and enterprise cyber operations.

What makes UpHold Aware's CNAPP different?

Unlike standalone CNAPP implementations focused primarily on cloud visibility, UpHold Aware CNAPP for Multicloud Federal Missions is designed as a mission-integrated operational capability aligned to the realities of federal cybersecurity environments.

Leidos combines cloud-native security analytics with operational mission context, helping organizations prioritize remediation efforts based on technical severity, mission impact, operational dependency and federal risk tolerance.

UpHold Aware's CNAPP is designed to support complex federal architectures that often extend beyond public cloud environments to include hybrid infrastructure, on-premises Kubernetes platforms, enterprise data centers and mission-specific enclaves. This broader operational perspective helps organizations maintain more consistent security visibility across interconnected environments.

The capability is also designed to integrate into existing federal cyber operations and governance processes, including:

- Security operations center (SOC) workflows
- DevSecOps pipelines
- Zero trust initiatives
- Risk management framework (RMF) processes
- Federal compliance and audit activities

Rather than treating cloud findings as isolated technical alerts, UpHold Aware's CNAPP helps organization correlate posture, workload, identity, and exposure risks into a more operationally relevant understanding of enterprise risk.

The mission-aware approach is intended to help federal programs:

- Focus remediation efforts on systems most critical to mission execution
- Reduce alert fatigue through operational risk prioritization
- Improve coordination across cyber, infrastructure and development teams
- Support more scalable cloud security operations across multicloud and hybrid environments

By integrating cloud-native technologies, including Wiz, within a broader federal operational framework, Leidos delivers a CNAPP capability designed to align cloud security outcomes with mission resilience and operational readiness.

Integrated risk prioritization

UpHold Aware CNAPP correlates posture, vulnerabilities, identity and exposure. Leidos helps the prioritization reflect:

- Mission criticality
- Operationally relevant impact
- Federal risk tolerance

Accelerated time to remediation

UpHold Aware's CNAPP helps agencies accelerate remediation by correlating cloud risk with operational ownership, workflow integration and mission priorities.

- Ownership clarity
- Workflow integration
- Measurable remediation outcomes

Rapid deployment, scalable operations

The platform's agentless model supports rapid onboarding. Leidos supports:

- Seamless integration into existing environments
- Alignment with federal architectures

- Long-term operational sustainability

Mission scenario: From fragmented alerts to actionable risk

Imagine a federal program deploys a cloud update introducing:

- Increased network exposure
- A vulnerable container image
- Over-permissive identity access.

These risks are often disconnected across tools.

Integrated operational response

When CNAPP is properly implemented, it is designed so:

- Aware's CNAPP correlates the risks into a single attack path
- Leidos aligns the resulting findings to mission systems and operational priorities
- Integrated workflows support rapid triage, ownership assignment and remediation coordination

Under these ideal conditions, the results should include:

- Faster understanding of risk
- Reduced alert fatigue
- Accelerated, mission-focused remediation
- Security teams with a clearer understanding of which issues represent meaningful operational risk

Forward with Leidos

Leidos brings decades of experience delivering cybersecurity solutions for highly regulated federal environments. UpHold Aware CNAPP incorporates modern cloud-native analytics and agentless visibility technologies, including Wiz, designed for multicloud scale.

UpHold Aware's CNAPP is designed to deliver:

- Unified multicloud visibility
- Context-driven risk prioritization
- Operationalized CNAPP aligned to federal missions

This combined approach helps agencies secure cloud environments and is designed to reduce drag on modernization efforts.

Conclusion

Federal agencies require more than visibility into cloud risk; they require the ability to understand which risks matter most to mission execution. UpHold Aware is designed to provide that mission-aware perspective by combining cloud-native CNAPP capabilities with Leidos operational expertise, federal architecture integration and risk-informed remediation workflows.

By leveraging technologies, including Wiz, within the broader operational framework, Leidos helps agencies reduce complexity, accelerate remediation and strengthen resilience across multicloud environments.