White Paper

Achieving Zero Trust and FIPS Compliance with Buoyant and Rancher Government Solutions

RGS
Rancher Government Solutions

BUOYANT
Creators of LINKERD

Table of Contents

Executive Summary

Government agencies are under pressure to secure their digital infrastructure against emerging and increasingly sophisticated cyber threats. Vulnerabilities at multiple layers within government and military operations make establishing unfailing security and compliance standards critical. Adherence to federal frameworks such as the Federal Information Processing Standards (FIPS) and the Federal Risk and Authorization Management Program (FedRAMP) is essential to protect and encrypt all data, whether at rest or in transit, against unauthorized access. In addition to federal standards, the Zero Trust architecture model is reshaping security practices by requiring continuous verification of every user, device, and application.

Buoyant and Rancher Government Solutions (RGS) have partnered to provide an integrated solution that meets the U.S. government's stringent security and compliance standards. This partnership combines RGS' RKE2 Kubernetes distribution with the Buoyant Enterprise for Linkerd (BEL) service mesh, offering a streamlined solution that simplifies the compliance process, strengthens security measures, and accelerates authorization and deployment.

This white paper discusses the security and compliance challenges faced by government agencies, the importance of FIPS, FedRAMP, and Zero Trust, and how combining Rancher RKE2 and Linkerd effectively addresses security challenges. By adopting this integrated technology, government and military operations can future-proof their security posture, adapt to evolving federal standards, and mitigate advanced cyber threats to maintain resiliency and operational efficiency.

Current Security and Compliance Challenges in Government

Increasing cyber threats are forcing government agencies to consider new ways to secure their digital infrastructure. Vulnerabilities exist at multiple levels within government operations, and cyber-attacks are continually finding new ways to exploit these weaknesses. To counter these threats, stringent security and compliance standards have been established at the federal level. These standards ensure government data remains protected and operations continue without disruptions.

Federal agencies must adhere to frameworks such as the Federal Information Processing Standards (FIPS) and the Federal Risk and Authorization Management Program (FedRAMP). These frameworks set requirements for cryptographic modules and cloud services, ensuring that all data, whether at rest or in transit, is adequately protected and encrypted against unauthorized access. Additionally, the Zero Trust model is changing security practices by assuming that threats can exist both inside and outside the network. This

paradigm requires continuous verification of every user, device, and application attempting to access resources, strengthening the security posture of government agencies.

Failing to comply with these standards can have severe repercussions. For example, massive data breaches that expose the sensitive personal information of millions of current and former federal employees, citizen information, and mission-critical data can be compromised in instances of inadequate security measures.

According to a 2024 report by the Government Accountability Office (GAO), federal agencies reported **over 30,000 information security in fiscal year 2022. Even more surprising is that agencies have not implemented many of GAO's comprehensive cybersecurity strategies or oversight recommendations despite the risks associated with inadequate cybersecurity processes. Until agencies implement robust cybersecurity practices, they will remain vulnerable to cyber threats and will be limited in their efforts** to comply with federal standards.

The Role of FIPS, FedRAMP, and Zero Trust in Government Compliance

Compliance with FIPS, FedRAMP, and Zero Trust principles is fundamental to safeguarding national security. These standards and principles form the foundation of a secure and compliant government technology infrastructure.

Importance of FIPS for Government Agencies

The Federal Information Processing Standards (FIPS) are a set of officially announced standards developed by the National Institute of Standards and Technology (NIST) for use in computer systems by non-military government agencies and government contractors. FIPS standards are designed to maintain the security and integrity of sensitive government data.

FIPS 140-2, the most widely recognized standard within this framework, focuses on security requirements for cryptographic modules, including hardware and software components that perform encryption and decryption functions.

Adherence to FIPS is critical for government agencies as it requires that cryptographic processes meet rigorous standards for data protection. By complying with FIPS, federal information systems maintain secure and reliable cryptographic activities.

The Need for FedRamp for Cloud Services

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that offers a standardized approach to security assessment, authorization, and continuous monitoring of cloud products and services. Complying with FedRAMP's

standards means cloud services used by federal agencies must meet strict security requirements to protect federal data and infrastructure.

Obtaining a FedRAMP Authorization to Operate (ATO) is a critical step in gaining the trust and business of federal agencies. This authorization signifies that a provider's services have been thoroughly vetted and meet high security standards, including implementing NIST SP 800-53 security controls.

Zero Trust: The Emerging Government Security Paradigm

Zero Trust is a federal strategy developed by the White House Office of Management and Budget (OMB) and initially introduced in January 2022 via Executive Order (EO 14028). It is a security model based on the principle of "never trust, always verify." Unlike traditional security approaches relying on perimeter defenses, Zero Trust assumes threats can originate both outside and inside the network. Therefore, every access request must be authenticated and authorized, regardless of origin.

The U.S. government has been a strong proponent of Zero Trust, with the OMB setting a deadline for civilian agencies to implement Zero Trust architectures by September 2024. This shift toward continuous verification and access controls is driven by the need to mitigate advanced persistent threats (APTs) and protect sensitive information.

A Better Together Solution

Government agencies face the dual challenge of achieving compliance and maintaining security while managing performance and operational efficiency. Failure to comply with security requirements such as FIPS and FedRAMP can lead to security breaches, data loss, and legal consequences. Traditional security models that rely on perimeter defenses are no longer sufficient against more advanced cyber threats.

Buoyant and Rancher Government Solutions (RGS) have joined forces to offer an integrated service mesh platform that meets the highest federal security and compliance standards. This combined solution simplifies the compliance process and bolsters overall security.

Introducing Buoyant Enterprise for Linkerd

Buoyant Enterprise for Linkerd (BEL) is the enterprise distribution of Linkerd, the popular open source service mesh, which provides a secure networking layer for microservices. BEL enables FIPS-compliant encryption and a Zero Trust architecture, facilitating secure communication between services without requiring significant changes to existing applications.

Key features of Linkerd include:

FIPS-Validated Cryptographic Modules

Linkerd uses cryptographic modules that are validated under FIPS standards. Specifically, it uses the BoringCrypto module certified under CMVP certificate 3678. This means all cryptographic operations, like encryption, decryption, key management, and digital signatures, meet the highest security standards of integrity and confidentiality mandated for federal information systems. It simplifies compliance for government agencies, providing peace of mind that their data is protected against sophisticated cyber threats.

Automation Encryption

Linkerd uses mutual TLS (mTLS) for all service-to-service communications to encrypt data moving between microservices. This encryption process is transparent to developers, meaning they don't need to change their application code.

This automatic encryption addresses a critical requirement of FIPS and FedRAMP, providing secure data transmission across the network. This feature is particularly valuable in distributed systems where microservices interact frequently, consistently protecting sensitive information against interception and unauthorized access.

Zero Trust Implementation

Linkerd supports the Zero Trust security model, which requires continuous verification of every access request. It mandates that every network call between services is authenticated and authorized, regardless of where it comes from.

This authentication extends down to specific HTTP paths or gRPC methods, providing fine-grained control over access policies. This continuous verification helps prevent unauthorized access and data breaches.

Memory Safety with Rust

Linkerd uses Rust programming language for critical data-handling components. Rust is known for its memory safety, which helps avoid common vulnerabilities in other programming languages like C and C++. Memory safety prevents common security issues in applications, such as buffer overflows and use-after-free errors, which attackers often exploit.

By building data path components in Rust, BEL establishes both a secure and performant service mesh.

Service Discovery and Load Balancing

Linkerd automates the discovery of services and the distribution of network traffic. This helps improve the performance and reliability of applications by routing requests optimally and using resources effectively.

The service discovery feature allows services to dynamically register and deregister, making scaling and updates seamless. The load balancing mechanism spreads traffic evenly across available instances, preventing any single instance from becoming a bottleneck.

Failure Recovery

Linkerd includes mechanisms to help services continue to operate even in the event of a failure. This improves the resilience and reliability of applications running within the service mesh.

Linkerd's failure recovery capabilities include automatic retries, circuit breaking, and health checks, which detect and mitigate failures in real time to maintain the system's stability and minimize downtime.

Authorization Policies

Linkerd provides fine-grained access control through its authorization policies, allowing administrators to define and enforce security policies for accessing services and APIs. This approach restricts interaction with sensitive resources to only authorized users and applications.

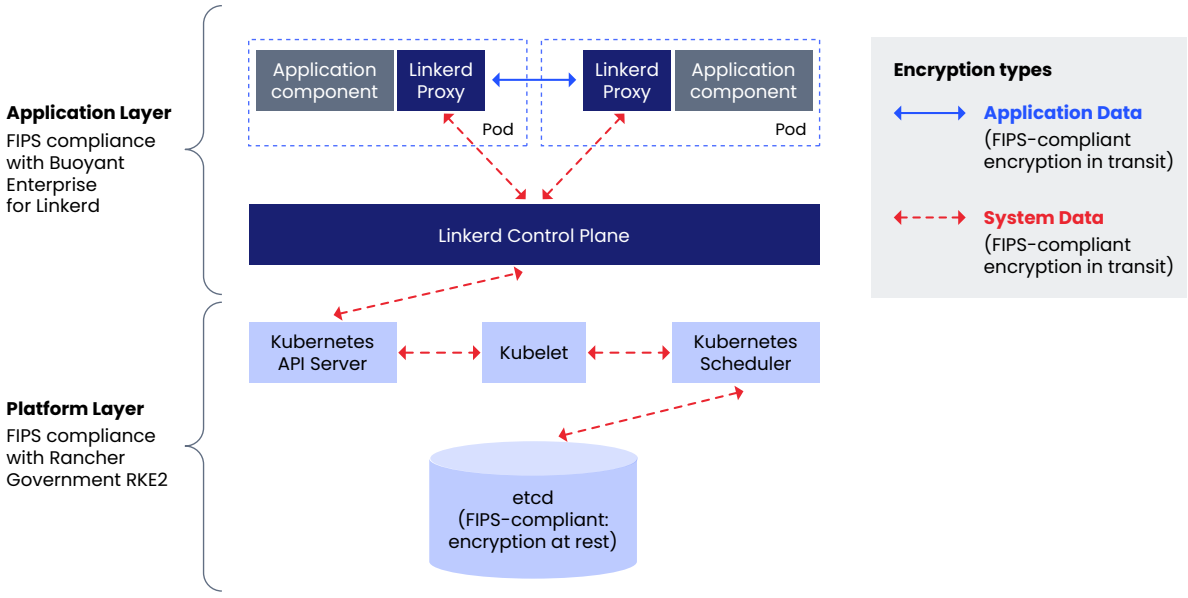
Linkerd's authorization framework integrates with existing identity and access management systems, providing centralized control over access policies and maintaining consistent security across the entire microservices architecture.

Rancher RKE2: Driving Compliance for Buoyant Enterprise for Linkerd

RGS' RKE2 is designed to meet the stringent compliance requirements of the U.S. government. Combining the best features of Rancher Kubernetes Engine (RKE) and Rancher K3s, RKE2 delivers a secure, easy-to-operate platform for various deployment environments, including on-premises, cloud, and edge.

RKE2 complies with DISA STIG validation, adhering to the strict security guidelines essential for the Department of Defense and other federal entities. It is also the first and only distribution with FIPS-140-2 certification, using cryptographic modules that conform to NIST standards to establish secure operations within Kubernetes environments.

Despite its advanced security features, RKE2 is designed for easy installation and operation. It offers pre-configured defaults and customizable options, allowing administrators to deploy and manage secure Kubernetes clusters quickly. RKE2 supports secure implementation across diverse environments, making it suitable for any environment.



Advantages of a BEL and RGS Partnership

The partnership between Buoyant and Rancher Government Solutions offers a powerful, integrated solution that provides improved security, streamlined compliance, and operational efficiency for government military operations. This combination offers several competitive advantages validated by current users, including:

Streamlining Compliance

Achieving FedRAMP Authorization to Operate (ATO) and maintaining FIPS compliance can be resource-intensive and time-consuming. Delays in compliance can block operational efficiency and expose agencies to security risks. Buoyant and RGS address these challenges by providing an out-of-the-box solution that simplifies and accelerates the compliance process.

Linkerd's FIPS-compliant encryption meets FedRAMP requirements for data in transit, reducing the effort needed for authorization. RKE2's secure, certified Kubernetes distribution adheres to DISA STIG and CIS Kubernetes Benchmarks to streamline the deployment and management process. This combination allows government agencies to achieve and maintain compliance efficiently without losing focus on their core missions.

In addition to these mandated security standards, Linkerd helps agencies meet Zero Trust architecture principles. Traditional security models rely solely on perimeter defense and are inadequate for modern cyber threats as they leave agencies vulnerable to internal and external attacks. Linkerd and RKE2 implement a Zero Trust framework that continuously monitors and protects IT infrastructure.

With continuous authentication and authorization for every network interaction, Linkerd ensures that only verified entities can communicate within the network. This approach aligns with OMB's Zero Trust model by providing security across all communication channels.

RKE2 supports this Zero Trust approach by default, securing all Kubernetes operations and allowing government agencies to continuously monitor and protect their IT infrastructure against advanced cyber threats.

Simplifying Development

Security and compliance complexities often burden developers, diverting their focus from core development tasks. Traditionally, managing encryption and security infrastructure required extensive effort and specialized knowledge. Linkerd abstracts these complexities, automating the processes to provide built-in security features that operate transparently.

Automating secure communication and compliance processes reduces the burden on developers so they can concentrate on creating applications that deliver business value. By handling the heavy lifting of security and compliance, Linkerd integrates security directly into the application architecture to improve productivity and accelerate development cycles.

Adaptability, Scalability, and Flexibility

Security standards are continuously advancing, requiring updates to maintain compliance. Failure to adapt to new standards can result in non-compliance with federal regulations and lead to security vulnerabilities. Buoyant and RGS are committed to keeping Linkerd and RKE2 compliant with changing standards.

Linkerd's FIPS-validated cryptographic modules are designed for easy updates to meet new requirements, reassuring agencies that they remain protected without significant infrastructure overhauls. It is designed to scale seamlessly with the growth of applications. It supports deployments across various environments, including on-premises, cloud, and edge, providing the flexibility to meet diverse operational requirements.

Linkerd's scalable architecture also allows it to handle increased loads without compromising performance. Its flexible deployment options enable agencies to adapt to changing needs and optimize resource utilization, ensuring the service mesh can grow with evolving security standards.

Key Takeaways

Government agencies face escalating cyber threats, making adopting an integrated security solution that meets federal compliance standards imperative. The partnership

between Buoyant and Rancher Government Solutions offers a robust, secure, and compliant technology solution that addresses these urgent needs.

The integration of RKE2 and Linkerd provides a unified platform that simplifies compliance, enhances security, and supports a Zero Trust architecture. In the face of advanced cyber threats, this integrated service mesh solution drives deep security, streamlined compliance, and operational efficiency so government and military operations can confidently focus on their core missions.

Competitive advantages of this partnership include:

Strengthened Security	End-to-end encryption, continuous authentication and authorization, memory-safe data handling.
Simplified Compliance	Built-in support for FIPS and FedRAMP reduces time and cost for achieving ATO and maintaining compliance.
Operational Efficiency	Allows developers to focus on business logic, enhancing productivity and accelerating development cycles.
Future-Proofing	Adapts to evolving standards, ensuring ongoing compliance through continuous innovation.
Flexibility and Scalability	Supports secure deployments across diverse environments, including on-prem, cloud, and edge.

Linkerd is designed to meet the demands of government and military IT environments by offering flexibility and scalability across deployments. With RKE2 and Linkerd, agencies can achieve a future-proof security posture, adapt to new standards, and mitigate advanced cyber threats. Implement this integrated technology today to remain resilient and secure no matter your mission.

About Rancher Government Solutions

Rancher Government is explicitly designed to address the unique security and operational needs of the U.S. Government and military as it relates to application modernization, containers, and Kubernetes.

Rancher is a complete open-source software stack for teams adopting containers. It addresses the operational and security challenges of managing multiple Kubernetes clusters at scale while providing DevOps teams with integrated tools for running containerized workloads.

Rancher Government supports all Rancher products, with U.S.-based American citizens supporting programs across the Department of Defense, the Intelligence Community, and civilian agencies.

About Buoyant

Buoyant is a U.S.-based company created by infrastructure engineers who defeated the notorious “fail whale” errors at Twitter. Buoyant’s mission is to provide truly future-proof and best-in-class security, observability, and reliability for Kubernetes platforms.

Buoyant is the creator and maintainer of Linkerd, the open-source, graduation-tier Cloud Native Computing Foundation service mesh. Buoyant’s enterprise software powers critical production infrastructure for leading organizations around the world, from 911 call centers to worldwide gaming applications to critical life-saving medical devices.

For more information, visit buoyant.io.