Teleport

Accelerate FedRAMP Authorization with Teleport

Contents

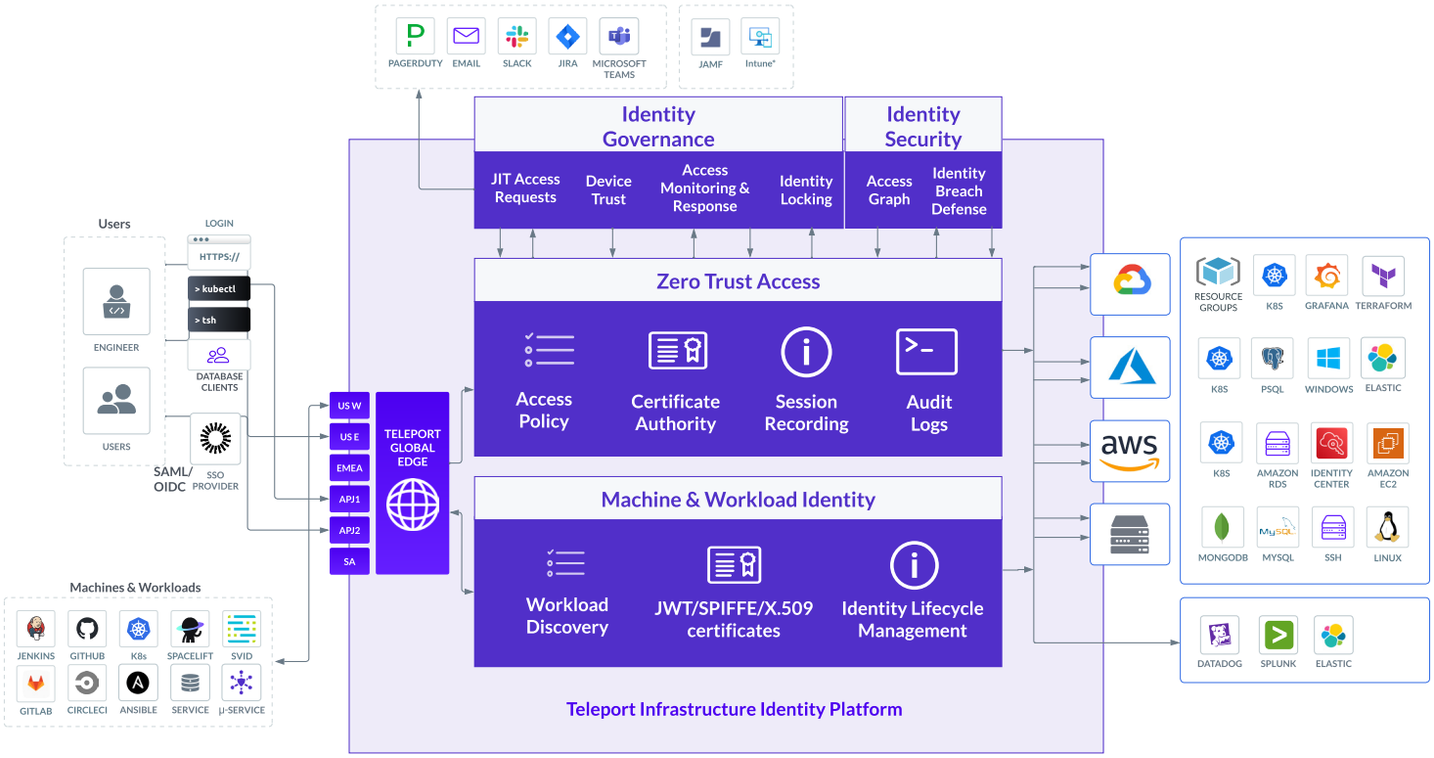
Introduction

FedRAMP Authorization can dramatically accelerate a company's growth by opening up market opportunities with the world's largest single buyer of Software as a Service (SaaS) products, the United States Federal Government. However, when rolling out access controls to meet FedRAMP compliance requirements, organizations of all sizes encounter significant challenges that can strain technical resources, escalate costs, and disrupt time-to-market goals. The stringent set of requirements related to infrastructure access control and auditing are frequently cited as some of the most difficult controls to achieve in the FedRAMP compliance process, presenting a substantial burden on engineering, security and compliance teams.

Navigating these complexities demands a robust and efficient solution for modern infrastructure access. Teleport is a critical ally for organizations embarking on the FedRAMP journey as well as those that are already FedRAMP Authorized and want to ease the burden on engineering and reduce the risk of ongoing audits.

With Teleport, FedRAMP administrators can easily demonstrate compliance with some of the most challenging controls for the Access, Identification, Authentication, and Audit categories. This significantly reduces the time required to achieve FedRAMP authorization and expedites the organization's time to market for federal-facing products.

This white paper describes how leading organizations use Teleport to achieve and maintain FedRAMP compliance and pass audits with flying colors. This paper illustrates a fictional example of the FedRAMP compliance process, comparing scenarios with and without Teleport. Through this narrative, readers will gain insights into how Teleport can streamline their compliance journey, making the path to authorization smoother and more efficient.



Teleport Infrastructure Identity Platform

The Teleport Infrastructure Identity Platform is an on-prem, self-service solution that runs inside your FedRAMP boundary to deliver on-demand, least-privileged access to infrastructure on a foundation of cryptographic identity and zero trust, with built-in identity security and policy governance. The Teleport Infrastructure Identity Platform improves productivity for engineers and operations teams, makes infrastructure resilient to bad actors or human error, and delivers fast, accurate reporting for compliance audits.

Teleport's modern architecture provides access to all of your team's critical internal resources through one standardized, simplified, and secured process. With Teleport, you can eliminate ad hoc, bespoke, error-prone access systems built by different teams with a central solution that engineers will love. The platform is simple to deploy and effortless to scale — allowing you to provide centralized access to thousands of hosts while freeing your administrators up to focus on other duties. With Teleport, your engineering, security, and compliance teams benefit from fine-grained access control across your services, which significantly increases security and visibility while decreasing effort, time, and risk.

The Challenges of Achieving FedRAMP Authorization: A Case Study of Acme Corp

Acme Corp is a fictional B2B software company specializing in employee productivity software.

It aims to secure federal contracts via a new product designed for federal agencies. With 500 employees, the company has a lean structure comprising Engineering, DevOps, IT, and a newly formed FedRAMP compliance team.

Acme Corp's infrastructure includes various access points and authentication methods:

Access and Authentication

- Key pairs created with AWS IAM installed on most bastion hosts for internal database access
- AWS SSM and Fleet Manager for terminal and remote desktop access
- Okta for Single Sign-On (SSO), roll-out underway

Auditing and Monitoring

- Basic logging via AWS CloudTrail
- Rolling out Sumo Logic for SIEM

Infrastructure Components

- Kubernetes clusters, EC2 instances, ECS, RDS, Redis, Elasticsearch, Kinesis
- Separate environments for FedRAMP and IL4 (isolated VPCs per agency)

Company Overview

Industry: B2B Software for Employee Productivity

Size: 500 employees

Departments: Engineering, DevOps, IT, and a newly formed FedRAMP compliance team

Goals: Expand market by securing federal contracts

Future Requirements

- Eliminate reliance on bastions for database access
- Implement more detailed activity monitoring and auditing
- Deploy Teleport agents or utilize agentless approaches to secure resource access
- Plans to link access requests to JIRA for automated workflows
- Use of Sumo Logic for centralized log aggregation and reporting
- Capture detailed user activity monitoring once sessions are connected

Compliance and Auditing Challenges

The FedRAMP compliance process introduces significant hurdles for Acme Corp:

Authentication and Access Control

- The current use of AWS IAM key pairs on bastions are effectively a shared secret, making it difficult to attribute actions to a specific user.
- Okta for SSO provides identification of users but needs to be integrated across multiple services to demonstrate consistent access controls.
- Simplifying, standardizing, and securing access across various services, including databases and Kubernetes clusters, is a critical concern.

Monitoring and Auditing

CloudTrail logs and session monitoring provide only basic oversight. Acme Corp needs to know when and how users accessed the system, as detailed activity logs are necessary to meet FedRAMP standards. In their current state, they will not meet the FedRAMP requirements.

Performance Issues

The remote desktop solution through AWS SSM and Fleet Manager is not optimal, causing performance issues that consistently impacts engineering productivity and user satisfaction.

Resource Allocation

The burden on technical resources, especially within the relatively small, newly formed FedRAMP compliance team, is considerable. Balancing the demands of achieving FedRAMP authorization with ongoing operational needs strains the company's capacity and threatens meeting deliverable timelines.

Cost and Time-to-Market

The cost implications of deploying, configuring, and maintaining these controls, along with potential delays in time-to-market due to compliance hurdles, are significant concerns for Acme Corp.

Teleport engineers understand these challenges and the complexities that organizations like Acme Corp face in their journey toward FedRAMP authorization. The next sections of this white paper demonstrate how Teleport alleviates these burdens, simplifies compliance efforts, and expedites the path to market.

The Traditional Path to FedRAMP ATO: Challenges and Pain Points

Phase 1: Discovery

Without Teleport — Time: 2-4 weeks

Coordinating Across Teams to Identify Current Access Control Mechanisms

For Acme Corp's large, non-standardized infrastructure, the first phase involves a comprehensive audit of their current access control systems. The discovery process requires collaboration among the Engineering, DevOps, IT, and FedRAMP compliance teams to gather complete and accurate documentation across various implementations — some of which are used only by a single team, some are shared, some were inherited from other teams and have been modified over time.

Risks of Human Error and Incomplete Documentation

Given the variety of tools and methods used, ensuring all access mechanisms are correctly identified and documented is challenging. Incomplete or inaccurate documentation leads to significant setbacks in the centralized authentication project moving forward, further pushing out the FedRAMP compliance timelines. Along the way, gaps in documentation and inaccurate knowledge of how the access control systems are built and operated further delay the program.

With Teleport — Time: 0 weeks

No Discovery Needed

Acme has made the decision to use Teleport. No discovery is needed. Teams are notified that Teleport is being deployed and told they can continue using their existing access control mechanisms while the service is rolled out. Teams who are excited for Teleport over their existing ad hoc approach are given the opportunity to volunteer as early adopters.

Phase 2: Standardization

Without Teleport — Time: 4 weeks

Selecting a Standard Access Control Mechanism

Acme Corp needs to select a standardized access control mechanism that meets FedRAMP requirements. This involves evaluating the current systems and deciding whether to unify them under a single solution or to integrate them in a way that meets the compliance standards. None of the existing mechanisms meet all of the FedRAMP control requirements which will require additional engineering work on both the centralized service and all engineering teams who integrate with that service. The need for additional engineering complicates the selection process since it is unclear who would be responsible for the uplift work.

Challenges in Achieving Stakeholder Buy-In and Consensus

Reaching consensus among stakeholders from different departments—each with its own priorities and technical preferences—proves to be very difficult. The FedRAMP compliance team must align the goals of engineering, DevOps, and IT to ensure a unified approach that satisfies all requirements. The back-and-forth with each of the parties involved further delays the implementation timeline.

With Teleport — Time: 0 weeks

Consensus Can Wait Until Teleport is Proven

Standardization across teams can occur after Teleport has been proven effective, eliminating the need to reach a consensus beforehand.

Phase 3: Stand-Up

Without Teleport — Time: 10 weeks

Adapt, Build, Scale, and Document the Chosen Technology

Once a standardized access control mechanism is selected, Acme Corp must build and scale this solution across their infrastructure. This involves implementing the technical uplift needed to fully address FedRAMP requirements and prepare it to scale from team-specific to organization-wide, validate the configuration for compliance and security, and the necessary internal documents for engineering to consume the service.

With Teleport — Time: 4 weeks

Teleport is Deployed to be Scalable, Secure, Compliant

Acme admins deploy and configure Teleport to meet (and exceed) FedRAMP requirements in the service's centralized configuration — a one-time process by ACME admins that does not require additional engineering. The service is deployed on EKS with auto-scaling enabled which reduces the daily cost during the initial stand-up phase and positions the service to grow as teams on-board to the platform.

Phase 4: Stand-Up

Without Teleport — Time: 16 weeks

Planning Live Cut-Over to the New Access Control System

Executing a live cut-over to the new system involves moving users and services to the updated access control mechanisms. This step is critical and must be meticulously planned to avoid business disruptions. The planning is complicated by the need to account for multiple teams across multiple services and the time needed for those mechanisms to be fully tested in the dev and staging environments before going into production.

With Teleport — Time: 8 weeks

Teleport is Integrated Throughout the Infrastructure

Once the initial setup is complete, Acme Corp begins integrating Teleport across its entire infrastructure. This includes rolling out Teleport on EC2 instances, Kubernetes clusters, and database servers. The process is streamlined by leveraging existing tagging and automation tools like Terraform, ensuring that resources are quickly and accurately enrolled in Teleport.

Phase 5: Decommissioning Old Services

Without Teleport — Time: 12 weeks

Disabling Old Access Mechanisms While Maintaining Security and Compliance

After the new system is live, Acme Corp must carefully decommission old access mechanisms. This involves ensuring that no security gaps are introduced during the transition and that all legacy systems are securely retired. Teams are reluctant to fully decommission their existing access mechanisms and rely completely on the newly deployed centralized service.

With Teleport — Time: 2 weeks

Disable Old Services, Including VPNs, Without Impacting Security or Availability

With Teleport fully deployed and all engineering teams utilizing the service, Acme Corp can decommission their previous access control mechanisms. This includes pulling the plug on VPNs and shutting down legacy authentication systems. Teleport's comprehensive access control and auditing capabilities ensure that security and compliance are maintained throughout this process — many of the shutdown actions are captured as session recordings which some teams share amongst themselves to celebrate the end of their old, ad hoc services.

Phase 6: Troubleshooting and Support

Without Teleport — Time: Ongoing

Planning Live Cut-Over to the New Access Control System

Executing a live cut-over to the new system involves moving users and services to the updated access control mechanisms. This step is critical and must be meticulously planned to avoid business disruptions. The planning is complicated by the need to account for multiple teams across multiple services and the time needed for those mechanisms to be fully tested in the dev and staging environments before going into production.

With Teleport — Time: 8 weeks

Teleport Constantly Evolves

The Teleport Infrastructure Identity Platform continuously grows and evolves to meet the challenges of enterprises by embracing new technologies and seamlessly integrating it with their existing solutions. The service tracks FedRAMP requirements as they grow and change, ensuring the capabilities to meet (and exceed) compliance are available to users through a simple, centralized configuration. Adoption of new technologies are as simple as updating to the latest version of Teleport to enable integration with those access control mechanisms, allowing engineering to focus on innovation at scale without risking security or compliance.

Teleport's Benefits for Acme Corp.

Teleport's centralized service provides a suite of robust features that significantly simplify FedRAMP compliance for Acme Corp. **Access Control** is fortified through secure and manageable admin connections, eliminating the risks associated with shared credentials and break-glass accounts. By leveraging **FIPS-Validated Encryption**, Teleport ensures that all admin connections meet the highest security standards. Additionally, **Session Controls and Logging** are implemented to manage concurrent sessions, enforce timeouts, display login banners, and automatically terminate sessions when necessary. Comprehensive logging and session recording provide detailed audit trails, making it easy for Acme Corp to demonstrate compliance and maintain security standards throughout their operations.

Key Benefits of Teleport for FedRAMP Compliance

Teleport is currently deployed within the boundaries of multiple FedRAMP Authorized organizations.

Customers consistently cite these key Teleport benefits:

- **Access Control:** All admin connections to internal hosts are secured and managed through robust access control mechanisms.
- **FIPS-Validated Encryption:** Every admin connection uses FIPS-validated encryption, ensuring the highest level of security.
- **Elimination of Shared Credentials:** There are no shared passwords or break-glass credentials, reducing the risk of unauthorized access.
- **Session Controls:** Teleport implements complex requirements such as concurrent session control, session timeouts, login banners, and automatic session termination.
- **Comprehensive Logging:** Teleport logs all personnel access and includes session recording for SSH, providing an easy-to-produce and complete audit trail.

Conclusion

Teleport provides a robust foundation for meeting FedRAMP requirements, especially regarding infrastructure access. By supporting the Federal Information Processing Standard (FIPS) 140-2, Teleport ensures the highest level of security for cryptographic modules, aligning with US government standards. This document has illustrated how Teleport facilitates your company's journey toward FedRAMP authorization by streamlining access control and compliance processes.

Additionally, Teleport enables comprehensive collection, management, and governance of all security events across your entire infrastructure, ensuring consistent and demonstrable compliance. With Teleport, organizations can significantly accelerate their FedRAMP compliance timeline, freeing up resources and accelerating time-to-market. Experience these benefits firsthand by starting a free trial today and see how Teleport can transform your FedRAMP compliance process.