

Accelerate FedRAMP Authorization with Teleport



Contents

Introduction3

Teleport Access Platform.....3

The Challenges of Achieving FedRAMP Authorization: A Case Study of Acme Corp4

Use Cases and Infrastructure.....4

Access and Authentication:4

Auditing and Monitoring:4

Infrastructure Components:.....4

Future Requirements:.....4

Company Overview4

Compliance and Auditing Challenges5

The Traditional Path to FedRAMP ATO: Challenges and Pain Points6

Phase 1: Discovery6

Phase 2: Standardization.....7

Phase 3: Stand-Up.....8

Phase 4: Roll-Out9

Phase 5: Decommissioning Old Services10

Phase 6: Troubleshooting and Support11

Key Teleport Benefits for FedRAMP Compliance.....12

Conclusion13

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 Access Platform

The Teleport Access 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 Access 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

Company Overview

Industry: B2B Software for Employee Productivity

Size: 500 employees

Goals: Expand market by securing federal contracts

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

Use Cases and Infrastructure

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), currently being rolled out.

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).

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:

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.



Want to view more? Unlock the full PDF.

Fill out the form to unlock the full PDF.

