Data Sheet

Teleport

Teleport Policy

Unified management of access policies across your infrastructure

At a Glance

- Unifies access policies for infrastructure, including:
  - + Multi-cloud & on-prem
  - + Servers (SSH), Kubernetes, Applications, Databases, Windows Desktop, Clouds
- Combines user and machine access policy across the enterprise
- Prioritizes and manages access to critical resources
- Shows identities with the highest number of standing privileges

It takes threat actors only 62 minutes to pivot from an initial breach to the rest of your infrastructure. With Teleport Policy, you can stop threat actors in their tracks.[1]

[1] Crowdstrike 2024 Global Threat Report

Harden attack surfaces and thwart threat actors

Modern infrastructure has been adopted broadly to accelerate application delivery. However, its complexity – with containers and microservices deployed as elastic, dynamic, and ephemeral resources – makes the task of managing access, mitigating access risk, and managing policy challenging.

In addition, different tools are often used to manage access policy for on-prem infrastructure and cloud native infrastructure. This creates siloed access policy, backdoor access paths to resources, and weak access patterns — all of which can lead to a compromise.

Teleport Policy unifies the management of access policies across computing infrastructure for all types of identities: human, machine, and computing resources like Kubernetes, databases and services.

Teleport Policy enables you to view access paths and uncover risky access patterns in seconds, and provides fine-grained oversight of privileges and access policies across hybrid infrastructure. Questions that Teleport Policy can quickly answer:

- Who has access to a specific infrastructure resource or data?
- Which infrastructure resources does a specific user have access to?
- What access changes to critical resources have occurred?
- Which identities have the largest number of standing privileges?
- Are there indirect paths that give a particular user access to a resource?
- How did a particular user gain access to a particular resource?

> “Teleport Policy is an attractive auditing and security tool. When I’m going through an audit, I can generate a snapshot of our user access matrix, showing who has access or potential access, and what our escalation policy is. If we’re going through a foresenic analysis of an incident, I can generate an impact report and see what was exposed and what the blast radius is.
>
> — John Capps, VP Infrastructure, VIDA

Teleport Policy: Key Capabilities

Gain Deep, Comprehensive Visibility

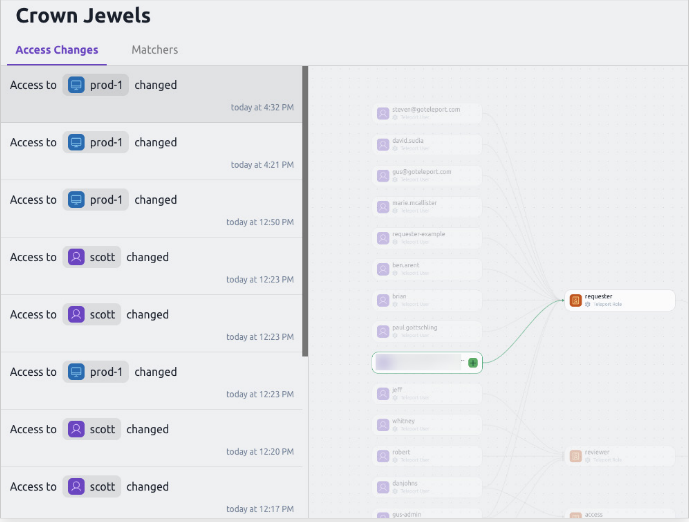
View unified, up-to-date relationships and policies between all identities, groups, and computing resources, enabling you to instantly uncover which human and non-human identities have access to what resource.

Discover SSH Keys and Access Patterns

Scan and discover SSH keys, enriching your access graph with a unified view of who has access to keys, and what access is enabled.

Prioritize Critical Resources

Mark critical infrastructure resources as crown jewels and track access changes to those separately.



Crown Jewels

Access to prod-1 changed
today at 4:32 PM

Access to prod-1 changed
today at 4:21 PM

Access to prod-1 changed
today at 12:50 PM

Access to scott changed
today at 12:23 PM

Access to scott changed
today at 12:23 PM

Access to prod-1 changed
today at 12:23 PM

Access to scott changed
today at 12:20 PM

Access to scott changed
today at 12:17 PM

***Crown jewels:** Mark critical infrastructure resources so you are immediately notified if access permissions change.*

Eliminate Shadow and Risky Access

Uncover shadow and risky access patterns, with full-stack analysis using SQL query. Strategically analyze and refine access paths to proactively eliminate potential risks and fine-tune privileges and access behavior.

Unify Governance and Compliance

Manage policy across your infrastructure in one place. Get rid of esoteric, discrete forms and templates and standardize query language with SQL.

Manage Policy Across Multiple Clouds

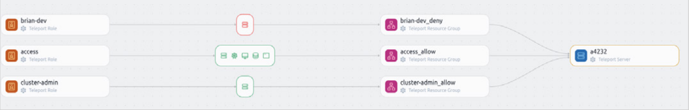
Manage policy across your AWS and Azure cloud environments, unifying policy across multiple clouds.

Integrate with Identity Providers (IdP)

Integrate with Okta and Entra ID, governing policy from one place for both human and non-human identities.

Identify Potentially Risky Identities

Quickly locate identities with the highest number of standing privileges.



***Risky identities:** In this example, Teleport Policy shows that developers normally only have access to developer resources as defined by 'devonly' policy. However, user 'tyler' has access to a production server 'se-ag-prod', a potential policy violation for the organization.*

Teleport

For more information please visit goteleport.com/platform/policy

About Teleport

Teleport is the global provider of modern access to infrastructure, improving efficiency of engineering teams, fortifying infrastructure against bad actors or error, and simplifying compliance and audit reporting. The Teleport Access Platform delivers on-demand, least privileged access to infrastructure on a foundation of cryptographic identity and zero trust, with built-in identity security and policy governance.

To learn more, visit goteleport.com.