AUTOMATE PROVISIONING, APPROVALS,
ACCESS REVIEWS, AND MONITORING FOR INFRASTRUCTURE AT SCALE

Teleport

Teleport Identity Governance

Streamline access requests

Accelerate engineering velocity and eliminate standing privileges with on-demand ephemeral access

Accelerate access reviews

Reduce compliance burden with role-based access lists that eliminate manual workflows and improve audit efficiency

Centralize governance

Identify weak access patterns, lock compromised users, add device trust, and provision/deprovision users.

Engineering velocity suffers when teams wait for access approvals

Complex infrastructure demands agile identity governance, but manual approval processes create bottlenecks. Cumbersome compliance workflows further impede efficient access reviews, creating security risks and slowing development. Task-based, short-lived privileges with automated workflows streamline compliance and accelerate engineering — eliminating waiting periods, generating comprehensive audit trails, and reducing the attack surface.

Teleport Identity Governance brings full lifecycle automation and access control directly to the engineering stack, unifying provisioning, access, approval, and continuous monitoring across humans, machines, workloads, and AI agents.

Teleport Identity Governance eliminates always-on privileged access by issuing ephemeral access issued on a just-in-time basis collapsing the attack surface by eliminating long-lived credentials and secrets sprawl. Teleport also automates the repetitive work of access reviews and makes them faster, clearer, and fully traceable — improving security posture, access control, and compliance requirements.

> "Teleport Access Requests changed the game in simplifying our infrastructure access for various compliances. It's led to more freedom and innovation by allowing us to move away from pre-defined root accounts."
>
> Erik Redding
> Director, Site Reliability Engineering
> Elastic

elastic

01
Least privileged access

02
Automated workflows

03
Hardened identities

Teleport Identity Governance solves these challenges by centralizing identity management, reducing the risk of unauthorized access, and ensuring organizations meet regulatory mandates like SOC 2, FedRAMP, and HIPAA. Real-time monitoring, automated access reviews, and policy enforcement eliminate weak access patterns and reduce attack surface. With identity as a primary attack vector for cyber threats such as phishing, credential theft, and privilege escalation, Teleport strengthens security by centralizing governance.

Key capabilities include just-in-time access, which grants only the necessary privileges to complete tasks, removing the need for always-on superuser accounts. Identity locking allows organizations to instantly revoke access for compromised accounts, minimizing the risk of insider threats and breaches. Device trust ensures that authorized users must pair with authorized devices to access sensitive infrastructure. Access lists define clear role boundaries and automate periodic reviews, satisfying compliance requirements without the manual ticketing burden that frustrates engineers.

Tightly integrated with Teleport Zero Trust Access and Teleport Machine & Workload Identity, Teleport Identity Governance provides a unified, scalable approach to securing both human and machine identities. By automating identity governance and enforcing consistent policies across diverse environments, it enhances security posture, streamlines compliance, and improves operational efficiency.

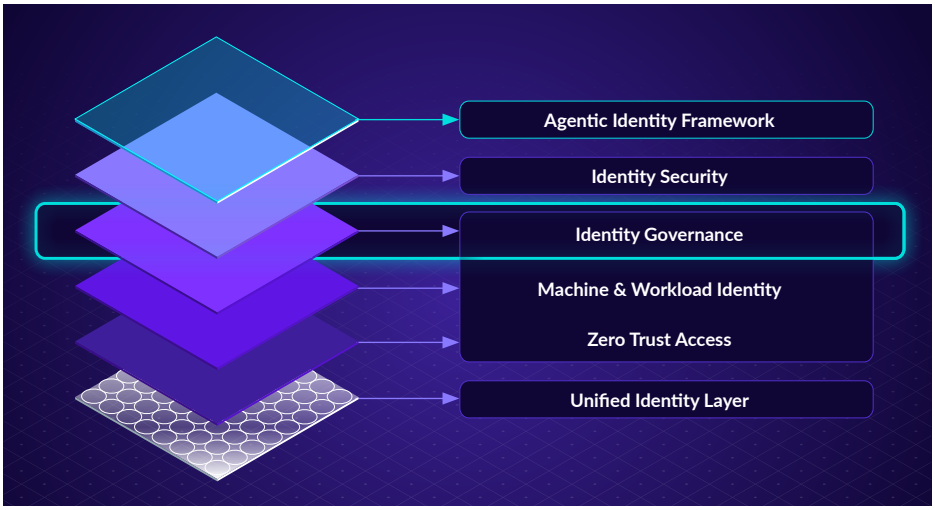
With Teleport Identity Governance, organizations can scale their infrastructure confidently and maintain desired security posture.

Key Capabilities

- **Just-in-Time Access Requests:** Grant only those privileges necessary to complete the task at hand. Remove the need for super-privileged accounts. Engineers can use their preferred tools — kubectl, ssh, ansible, postgresql and many more.
- **Automatic Access Requests & Approvals:** Automate pre-defined workflows based on RBAC, ABAC, or context-based authorization.
- **Access Lists & Access Reviews:** Review access requests using Slack, PagerDuty, Microsoft Teams, Jira and ServiceNow. Assign managers, automate mandatory reviews, and implement custom review logic using our API and Go SDK. Integrates with AWS Identity Center.
- **Session & Identity Locks:** Lock suspicious or compromised identities and stop all their activity across all protocols and services.
- **Device Trust:** Require an up-to-date, registered device for each authentication. Teleport uses TPMs and secure enclaves to give every device a cryptographic identity. Restrict further by resource or MDM-authorization.
- **User & Group Provisioning & Deprovisioning:** SCIM & Custom Protocols, including Okta and Entra.
- **Access Monitoring & Response:** Detect overly broad privileges and inspect sessions lacking strong protection such as multi-factor authentication or device trust. Alert on access violations and purge unused permissions with automated access rules.

Teleport Infrastructure Identity Platform

Teleport Identity Governance is part of the Teleport Infrastructure Identity Platform, which establishes a unified identity layer for humans, machines, workloads, and AI agents — all secured cryptographically. By making identity the foundation of trust, Teleport replaces fragmented identity and access management systems with scalable zero trust across complex cloud and on-premises infrastructure environments.



Get Started Today! Try Teleport for free 14-days at goteleport.com/signup | Request a call at goteleport.com/signup/enterprise

Teleport, the AI Infrastructure Identity Company, establishes a unified identity layer for humans, machines, workloads, and AI agents — preventing identity attacks, accelerating engineering, and enabling secure AI adoption. For more information, visit goteleport.com or follow @goteleport.

Teleport

Follow us on: