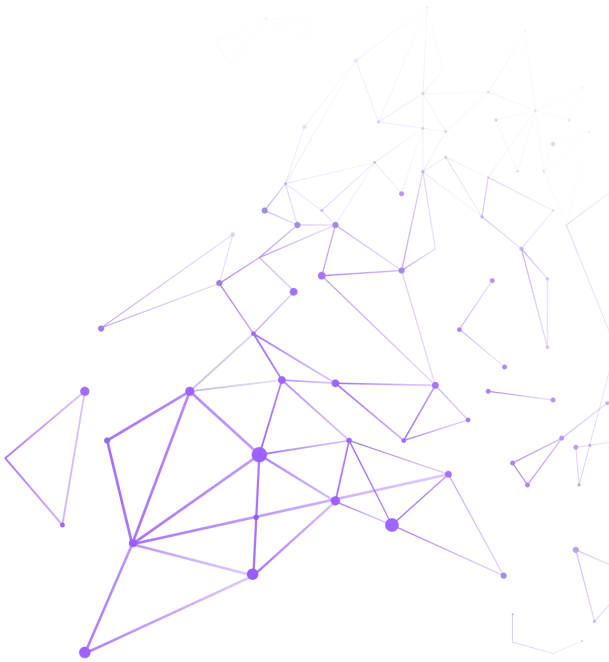


Teleport Enterprise Edition Pricing Guide

Revision: Jan 6, 2026

The Teleport Infrastructure Identity Platform modernizes identity, access, and policy for infrastructure, for both human and non-human identities, improving engineering velocity and resiliency of critical infrastructure against human factors and compromise.

Teleport

Overview

Teleport Infrastructure Identity Platform consists of four products:

- **Teleport Zero Trust Access**
  provides engineers with just-in-time, least-privileged access to applications, servers, databases, Kubernetes clusters, MCP servers, git repositories, and other resources across distributed infrastructures, improving engineering time to market and infrastructure resiliency.
- **Teleport Machine & Workload Identity**
  provides non-human identity management and access control, improving infrastructure resiliency by securing system and data access between machines and workloads.
- **Teleport Identity Governance**
  hardens and monitors identities for both human and non-human identities, improving resiliency of infrastructure from compromise due to human factor or identity attacks.
- **Teleport Identity Security**
  exposes and eliminates hidden risk across all of your infrastructure.

Teleport Zero Trust Access, Teleport Machine & Workload Identity, and Teleport Identity Governance are bundled together as our **Standard** offering for companies deploying access & governance use cases.

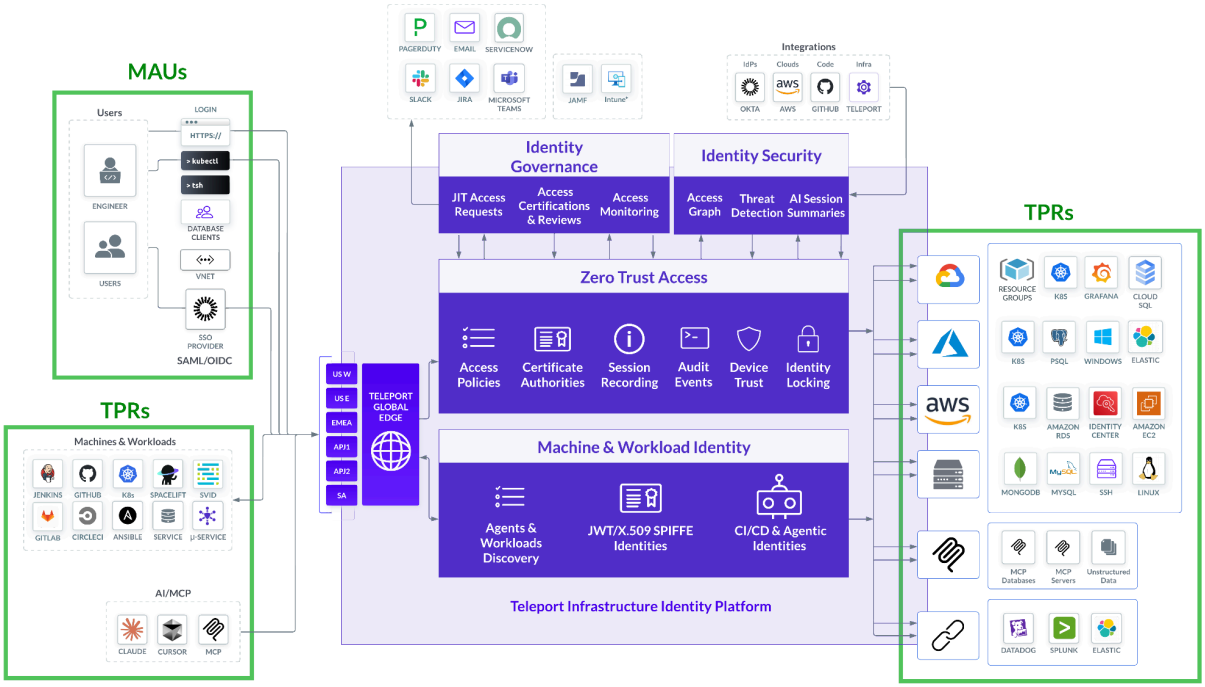
Our **Premium** offering adds Teleport Identity Security for companies that also want to deploy identity security use cases.

Teleport Infrastructure Identity Platform		
Enterprise Edition	**Standard**	**Premium**
Teleport Zero Trust Access	✓	✓
Teleport Machine & Workload Identity	✓	✓
Teleport Identity Governance	✓	✓
Teleport Identity Security	N/A	✓

Billable Metrics

Teleport Infrastructure Identity Platform pricing is based on usage, using two billable metrics:

Usage-Based Pricing	
Billable Metric	**Description**
Monthly Active User (MAU)	any unique interactive local or SSO user, utilizing any protocol or interface, who shows activity at least once within a monthly period, starting on the subscription start date and ending on each monthly anniversary thereafter. "Active" means a user having performed any activity that would appear in an audit; for example, connecting to a resource via the Web UI or via `tsh login`, submitting an access request and so on
Teleport Protected Resource (TPR)	any unique resource such as a Kubernetes cluster, SSH server, database instance, Windows Desktop, serverless endpoint, MCP server, git repository, or a machine or workload identity (any distinct CI/CD pipeline, machine host, microservice, or similar non-human identity) that has registered itself with the Teleport cluster at least once within a monthly period. We aggregate TPRs during each day on an hourly basis, and take an hourly average to compute a daily TPR. Then we average the daily TPR over a monthly period, which starts on the subscription start date and ends on each monthly anniversary thereafter



Teleport

Teleport Enterprise Edition

Teleport Enterprise Edition is Teleport's commercial edition of its Infrastructure Identity Platform. Teleport products are available as follows:

Products

Teleport Infrastructure Identity Platform			
Enterprise Edition	**Standard**	**Premium**	**Billable Metrics**
Teleport Zero Trust Access	✓	✓	• **MAUs** *(Monthly Active Users)* • **TPRs** *(Teleport Protected Resources)*
Teleport Machine & Workload Identity	✓	✓	
Teleport Identity Governance	✓	✓	
Teleport Identity Security	N/A	✓	

Support

Support Packages	Products	Notes
Priority Support	All products	Always included for self-hosted, hybrid and cloud deployments of the Teleport Platform.
Multi-Region High Availability Support	Enterprise Edition - Standard	Modifies Priority Support by elevating Level 1 Severity SLA from 1 hour to 30 minutes.

Deployment & Cloud Support Packages

Teleport can be deployed on-premises or in the cloud. For customers choosing Teleport-managed cloud deployment, Teleport offers two service packages:

- **Standard High Availability** is offered with Teleport-managed cloud deployments, featuring a 99.9% SLA with single-region failover and up to 50K connected resources per tenant.
- **Multi-Region High Availability** is Teleport-managed cloud deployment offering 99.99% SLA, up to 130K connected resources, and Severity Level 1 30 minute response time.

Support Service	Failover	Availability Zones	SLA	Connected Resources per Tenant	Fee	Tenants Included	Additional Tenant Cost	Max Tenants Allowed	Paired Support
Standard High Availability	Single Region	3	99.9%	Up to 50k	Included	2	Yes	10	Priority Support
Multi-Region High Availability (MRHA)	Multi Region	9	99.99%	Up to 130k	Yes	2	Yes	5	MRHA Support

Teleport

APPENDIX

Teleport Enterprise Edition Key Features

Teleport Infrastructure Identity Platform - Key Capabilities
Teleport Zero Trust Access
On-demand, least privileged access, on a foundation of cryptographic identity and zero trust.
• Zero-Trust access for SSH, RDP, Kubernetes, Databases, AWS, Azure, GCP API and CLI, Web applications and services, TCP endpoints, machine-to-machine access for Linux, Windows and MacOS, MCP servers and databases. • Issuing strong cryptographic identity and SAML/OIDC SSO with external identity providers and Teleport for every protocol - Kubernetes, SSH, Database and Windows Desktop. • Role-based access control and moderated sessions for each protocol • Controls for FedRAMP, PCI, SOC2, SOX, ISO, NIS2, DORA regulatory frameworks • Session recordings and structured audit logs for every session and request • Enhanced Session Recording with detailed kernel-level events for SSH protocol • Integrations: Infrastructure as Code (IaC): Terraform, K8, JamF, ServiceNow, Jira, HSM, KMS and 170+ other integrations. • VNet - virtual network emulation. • Identity Locking - block identity activity across the entire infrastructure. • Device Trust for client endpoint devices with JamF and Intune integrations.
Teleport Machine & Workload Identity
A product for non-human identity management and access control, improving infrastructure resiliency by securing system and data access between machines and workloads.
• Service Discovery: Live inventory of machine and workload identities for CI/CD jobs, microservices, agentic AI, and others • Secretless Authentication: Eliminates the need for API keys and long-term secrets • Ephemeral Authorization: With granular ABAC/RBAC for workload interactions • Auditability: Audit data, exportable to SIEMs, for compliance reporting & reviews • Integrations: Supports open-source policy agents, dev tool APIs, and bootstrapping trust with TPMs and Cloud IAM. Others include Jenkins, Github actions, Terraform Cloud, AWS Roles anywhere and more. • Open Standards - JWT, SPIFFE, x509 and others to avoid vendor lock-in

Teleport Identity Governance

Hardens and monitors identities for both human and non-human identities, improving resiliency of infrastructure from compromise due to human factor or identity attacks.

- Access requests and access lists with periodic access reviews, alerts, integrations with Pager Duty, JIRA, OpsGenie and other services.
- Automatic access reviews and access review rules.
- Okta Groups provisioning/deprovisioning and SCIM integration.
- Microsoft Entra ID directory synchronization and SSO integration.

Teleport Identity Security

Expose and eliminate hidden risk in your infrastructure, including suspicious identity behavior, shadow access, and blind spots.

- Access Graph - maps your access space as a unified graph.
- Import and analysis of AWS, Azure, Okta, Microsoft Entra, GitLab and AWS IAM roles.
- Detect and Alert on access change with Crown Jewel Alerting
- Discover shadow access with SSH Key Scanning
- Accelerate forensic investigation with context-based analysis in Identity Activity Center
- Streamline compliance with AI Session Summaries

Teleport

Machine & Workload Identity TPR examples

The Machine & Workload Identity agent, `tbot`, runs on your machines and issues short-lived credentials to your workloads providing them with an identity and allowing them to access other resources protected by Teleport. We count each unique instance of `tbot` as a TPR as determined by hourly average. Here are a couple of examples below:

Virtual Machine (1 TPR per VM): Each virtual machine that will run `tbot` as a long-lived background service to issue identities to services running upon that machine will count as 1 TPR.

Kubernetes Cluster (1 TPR per node): When using Kubernetes integration and SPIFFE workload attestation, the `tbot` agent runs as a daemon-set, and each node in K8S counts as 1 TPR.

CI/CD Pipeline (1/730th TPR per run): Each time the CI/CD pipeline runs, an unique ephemeral instance of `tbot` will spawn to issue an identity for that pipeline run. Assuming the pipeline run takes less than 1 hour, due to the hourly averaging mechanism used by Teleport, this counts as 1/730th of a TPR. If you had 730 CI/CD runs in a month, this would be 1 TPR.

Things that are **not counted** as TPRs:

- SPIFFE IDs
- X.509 certificates

Identity Security TPR examples

Every Teleport Protected Resource discovered for the purposes of Zero Trust Access is available and counted for Identity Security (when Identity Security is enabled) and vice-versa.

> As a rule of thumb, everything that is a computing resource or a bot with a virtual or real CPU and memory is a TPR, otherwise it's not.

Examples of resources visible in Identity Security that are not TPRs:

IAM roles, Okta groups, Entra ID groups:
These AWS and other SaaS resources are highly ephemeral. Identity Security may discover and reveal them in the access graph, but those are not counted as TPRs.

SSH Keys, end-user computers, Teleport Roles, RDS tables:
These are examples of other fine-grained resources that may be discovered by Identity Security, but those are not counted as TPRs either.

Machine and Workload Identity Jenkins jobs, Github actions and microservices:
Identity Security may discover and reveal them in the access graph, but those are not counted as a TPR for the purposes of Identity Security.