

Teleport Enterprise Edition Pricing Guide

Revision: Aug 13th, 2025

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.

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, and other resources across distributed infrastructures, improving engineering time to market and infrastructure resiliency.
- **Machine & Workload Identity** is a solution for 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.

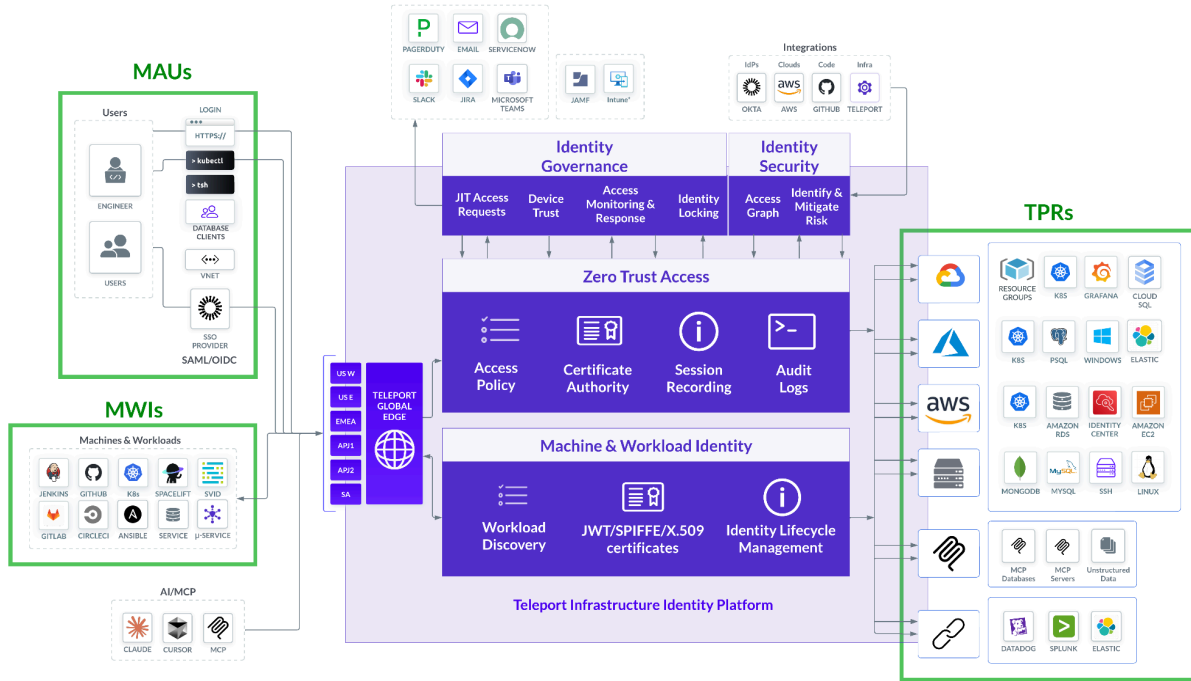
Billable Metrics

Teleport Infrastructure Identity Platform pricing is based on several billable metrics:

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. MAU is the primary billable metric of Teleport.

Teleport Protected Resource (TPR): any unique resource such as a Kubernetes cluster, SSH server, database instance, Windows Desktop or a serverless endpoint, 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.

Machine & Workload Identity (MWI) is any distinct CI/CD pipeline, machine host, microservice, SPIFFE ID or similar non-human-identity. We aggregate MWI during each day on an hourly basis, and take an hourly average to compute a daily MWI. Then we average the daily MWI over a monthly period, which starts on the subscription start date and ends on each monthly anniversary thereafter.



Teleport Enterprise Edition

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

Products	Billable Metric	Entitlements
Teleport Zero Trust Access	MAU - Primary Billable Metric	Always included. Sets base price for each MAU.
	TPR - Secondary Billable Metric	We include a certain amount of TPRs with each purchased MAU. Users can purchase extra TPRs over the included amount for a separate price for each TPR.
Teleport Machine & Workload Identity	MWI - Secondary Billable Metric	We include a certain amount of MWIs with each purchased MAU. Users can purchase extra MWIs over the included amount for a separate price for each MWI.
Teleport Identity Governance	MAU - Primary Billable Metric	Increases price for each MAU. We recommend Identity Governance Product for all Enterprise customers, with possible opt-out.

Teleport Identity Security	TPR - Secondary Billable Metric	Increases price for each TPR. Customers can opt-in to Teleport Identity Security.
Support Packages	Products	Notes
Multi-Region High Availability	Applies to Zero Trust Access, Identity Governance, Machine & Workload Identity products deployed in the cloud.	This offering requires a minimum standard contract value, calculated before HA and after discount. Increases price for each TPR and MAU for Zero Trust Access and Identity Governance.
Priority Support	All products	Always included for self-hosted, hybrid and cloud deployments of the Teleport Platform.
Enterprise Support	All products	Only Included with Multi-Region High Availability. See below for details.

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 and Multi-Region High Availability.

Multi-Region High Availability is a Teleport Platform deployed in Teleport-managed cloud, offering 99.99% SLA increase relative to standard's high availability 99.9% SLA, scaling up to 130K connected resources relative to standard's 50K connected resources and Enterprise support with global Severity Level 1 support times improved to 24/7 and 30 minutes response time, relative to the 1 hour response time in Priority we offer in Standard High Availability.

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	Multi Region	9	99.99%	Up to 130k	Yes	2	Yes	5	Enterprise Support

APPENDIX

Teleport Enterprise Edition Key Features

Product	Overview	Key Capabilities
Teleport Zero Trust Access	On-demand, least privileged access, on a foundation of cryptographic identity and zero trust.	<ul style="list-style-type: none"> • 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.
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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Access requests and access lists with periodic access reviews, alerts, integrations with Pager Duty, JIRA, OpsGenie and other services. • Access Monitoring and identity locking. • Device Trust for client endpoint devices with JamF integration. • Okta Groups provisioning/deprovisioning and SCIM integration. • Microsoft Entra ID directory synchronization and SSO integration.
Teleport Identity Security	Defend against identity breaches by revealing and eliminating shadow access and blind spots.	<ul style="list-style-type: none"> • 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

Machine & Workload Identity MWI examples

Jenkins job (1 MWI): A Jenkins job type that deploys a certain service is one MWI, as determined by hourly average of job executions. To estimate the amount of MWIs, count the number of different jobs in Jenkins.

Github action or Gitlab Pipeline (1 MWI): A github action type is one MWI, as determined by hourly average. For example, if a job or action runs every hour of the month, it would count as MWI. If a job or action runs half of the hours in the month, it will count 1/2 MWI. To estimate the amount of Github Actions MWI, look at the .github/actions folder in a repository..

Microservice or SPIFFE (SVID) (1 MWI): With a workload Identity support and SPIFFE, every microservice enrolled in Machine Workload Identity is one MWI, (as determined by hourly average, regardless of whether it starts and stops multiple times per day. To estimate the amount of MWIs in a K8s cluster, count the amount of different services.

Identity Security TPR examples

Teleport Identity Security and Teleport Zero Trust Access use exactly the same definition of TPRs.

Every 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.