Teleport

Open Security Summit Nov 12, 2021

Using Teleport to Secure SSH and Kubernetes Access

- Sakshyam Shah

Whoami

Sakshyam Shah

- Developer relations engineer @ Teleport
- Eight years in cybersecurity (been on both offensive and defensive side)
- Love talking about new technologies and startups

@sshahcodes

@sshahtweets

@sshahconnects

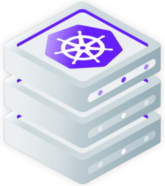
What is Teleport ?

Unified Access Plane

Teleport allows engineers and security professionals to unify access for SSH servers, Kubernetes clusters, web applications, and databases across all environments.

Server Access

For SSH servers

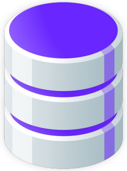


Kubernetes Access

For K8s clusters

Application Access

For web applications



Database Access

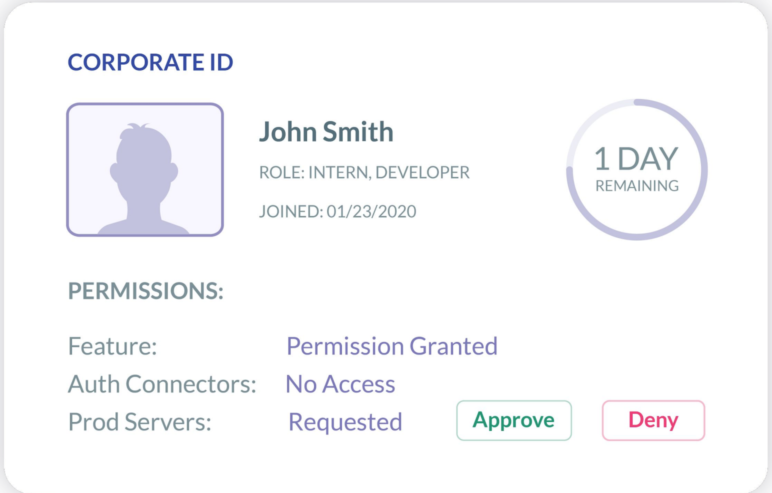
For databases

Teleport

EASILY IMPLEMENT SECURITY AND COMPLIANCE

IDENTITY CERTIFICATES

Allows users to retrieve their SSH credentials via your single sign-on (SSO) provider. Teleport supports all SAML/OIDC based SSO solutions.



CORPORATE ID

John Smith

ROLE: INTERN, DEVELOPER

JOINED: 01/23/2020

1 DAY REMAINING

PERMISSIONS:

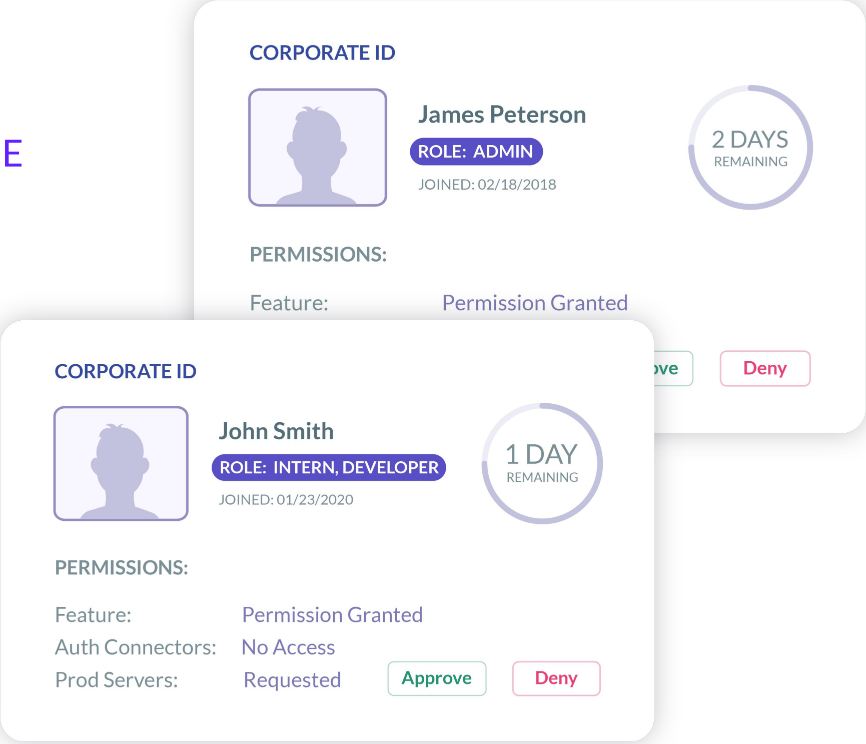
Feature:	Permission Granted
Auth Connectors:	No Access
Prod Servers:	Requested

Teleport

EASILY IMPLEMENT SECURITY AND COMPLIANCE

ROLE BASED ACCESS

Define User Roles and restrict each role to specific actions. RBAC also allows you to partition cluster nodes into groups with different access permissions.



CORPORATE ID

James Peterson
ROLE: ADMIN
JOINED: 02/18/2018

2 DAYS REMAINING

PERMISSIONS:

Feature: Permission Granted

ove Deny

CORPORATE ID

John Smith
ROLE: INTERN, DEVELOPER
JOINED: 01/23/2020

1 DAY REMAINING

PERMISSIONS:

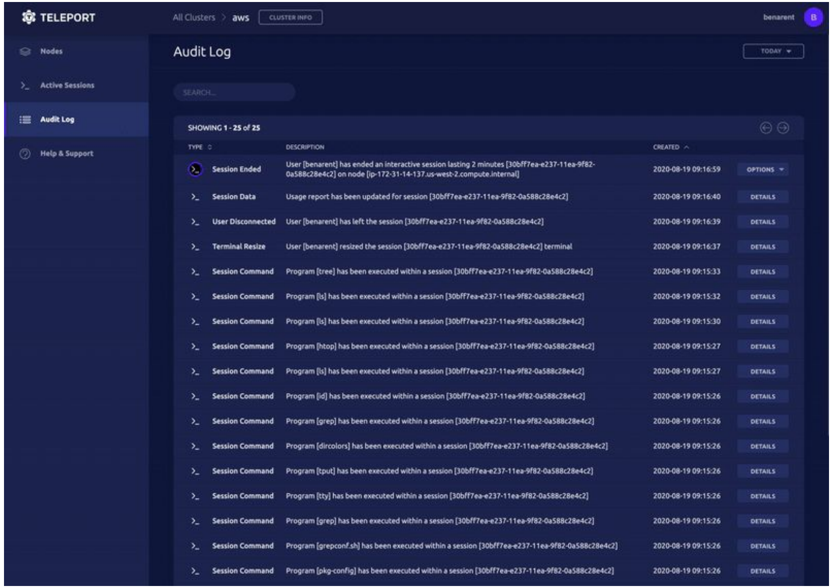
Feature: Permission Granted
Auth Connectors: No Access
Prod Servers: Requested Approve Deny

Teleport

COMPLETE VISIBILITY INTO ACCESS AND BEHAVIOR

COMPLETE SESSION VIEW

Teleport maintains a list of live sessions across all protocols and environments, providing an instant picture of what's happening. Each session is recorded and tied to identities of humans and machines involved.



Audit Log

SHOWING 1 - 25 of 25

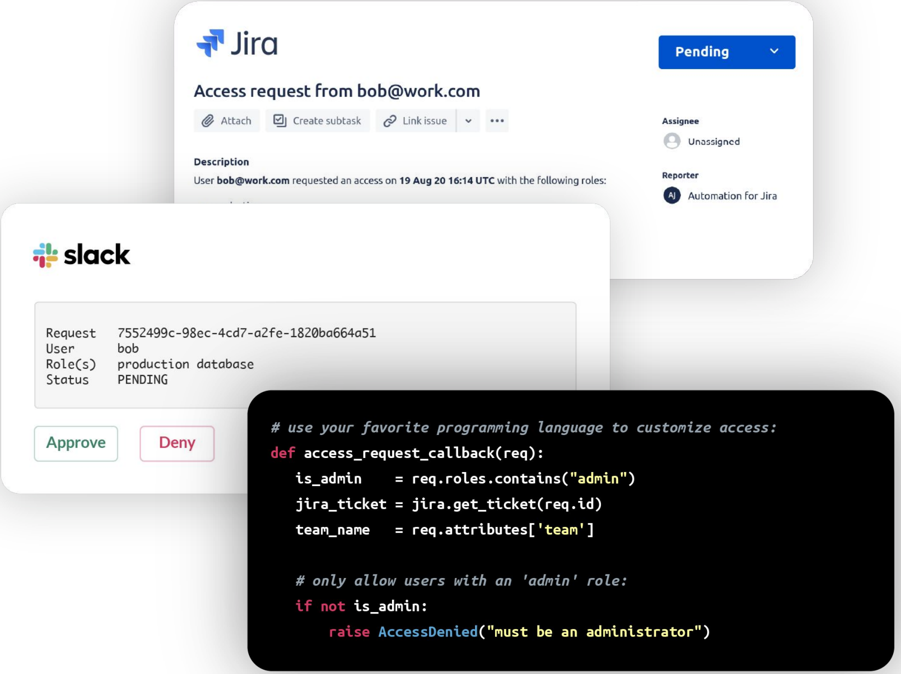
TYPE	DESCRIPTION	CREATED	
Session Ended	User [benarent] has ended an interactive session lasting 2 minutes [30bff7ea-e237-11ea-9f82-0a588c28e4c2] on node [ip-172-31-14-137.us-west-2.compute.internal]	2020-08-19 09:16:59	OPTIONS
Session Data	Usage report has been updated for session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:16:40	DETAILS
User Disconnected	User [benarent] has left the session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:16:39	DETAILS
Terminal Resize	User [benarent] resized the session [30bff7ea-e237-11ea-9f82-0a588c28e4c2] terminal	2020-08-19 09:16:37	DETAILS
Session Command	Program [tree] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:33	DETAILS
Session Command	Program [ls] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:32	DETAILS
Session Command	Program [ls] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:30	DETAILS
Session Command	Program [htop] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:27	DETAILS
Session Command	Program [ls] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:27	DETAILS
Session Command	Program [id] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:26	DETAILS
Session Command	Program [grep] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:26	DETAILS
Session Command	Program [dircolors] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:26	DETAILS
Session Command	Program [tput] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:26	DETAILS
Session Command	Program [tty] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:26	DETAILS
Session Command	Program [grep] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:26	DETAILS
Session Command	Program [grepconf.sh] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:26	DETAILS
Session Command	Program [pkg-config] has been executed within a session [30bff7ea-e237-11ea-9f82-0a588c28e4c2]	2020-08-19 09:15:26	DETAILS

Teleport

EASILY IMPLEMENT SECURITY AND COMPLIANCE

ACCESS REQUESTS

Grant minimal privileges by default. Approve or deny privilege escalation requests on-demand with ChatOps, Slack, PagerDuty, or programmable API.



Access request from bob@work.com

Description

User **bob@work.com** requested an access on **19 Aug 20 16:14 UTC** with the following roles:

Assignee

Unassigned

Reporter

Automation for Jira

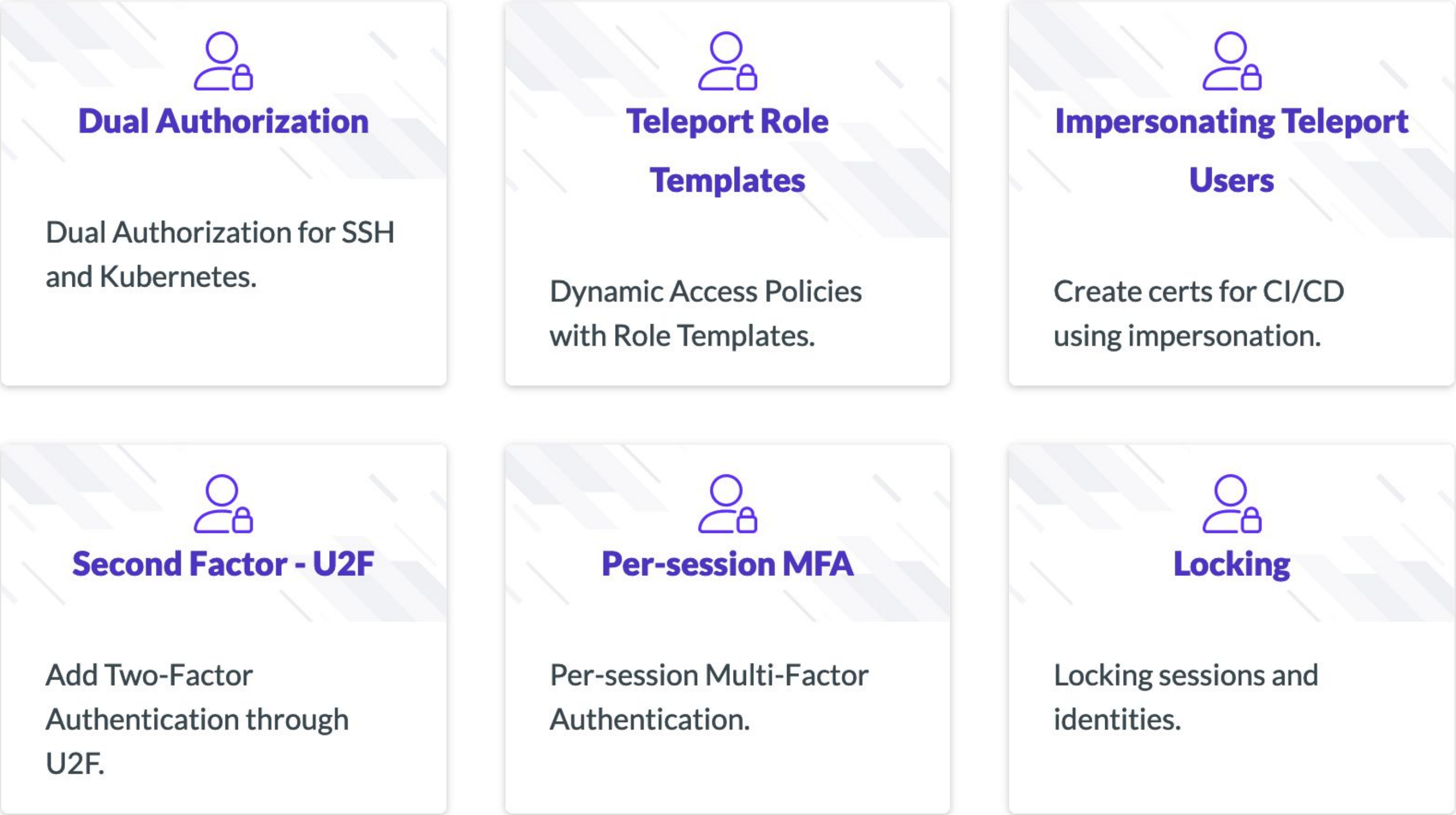
```
Request   7552499c-98ec-4cd7-a2fe-1820ba664a51
User      bob
Role(s)   production database
Status    PENDING
```

```
# use your favorite programming language to customize access:
def access_request_callback(req):
   is_admin     = req.roles.contains("admin")
   jira_ticket  = jira.get_ticket(req.id)
   team_name    = req.attributes['team']

   # only allow users with an 'admin' role:
   if not is_admin:
       raise AccessDenied("must be an administrator")
```

Teleport

Teleport Access Control



Dual Authorization

Dual Authorization for SSH and Kubernetes.

Teleport Role Templates

Dynamic Access Policies with Role Templates.

Impersonating Teleport Users

Create certs for CI/CD using impersonation.

Second Factor - U2F

Add Two-Factor Authentication through U2F.

Per-session MFA

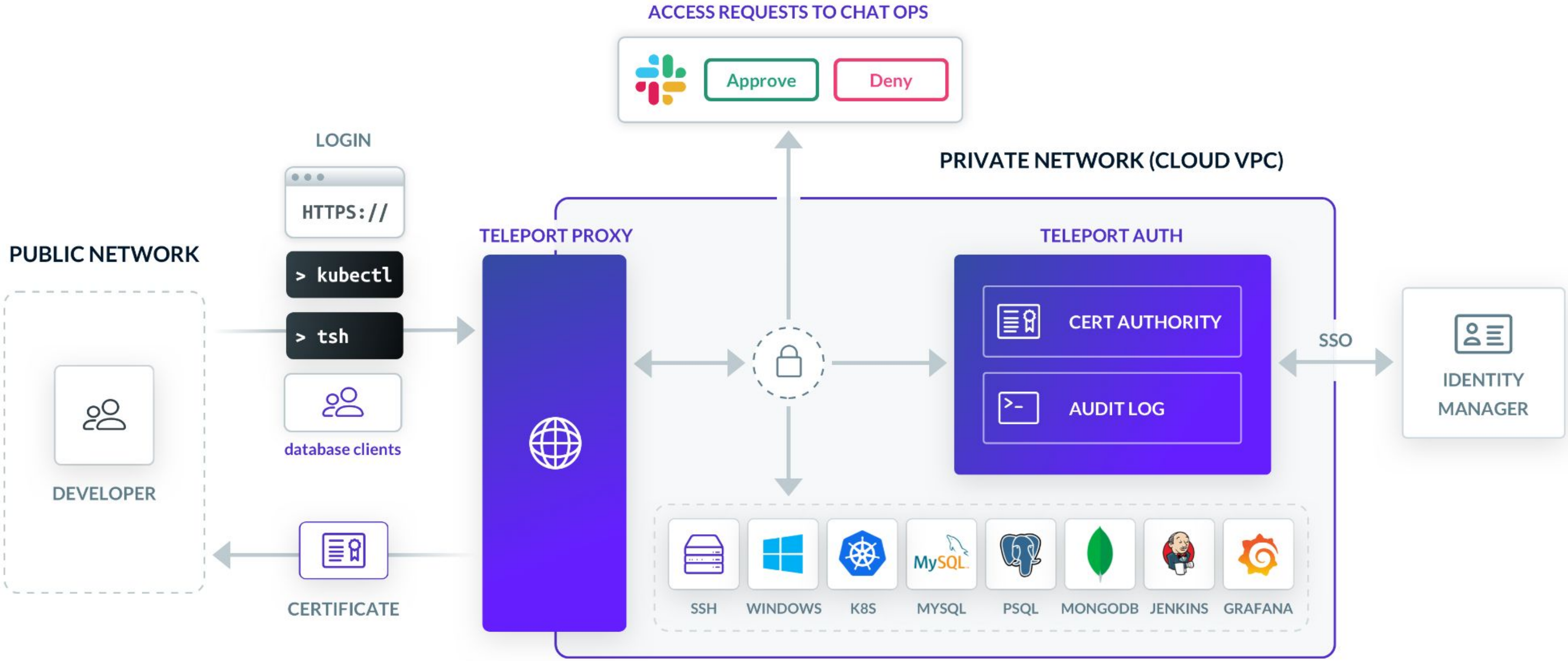
Per-session Multi-Factor Authentication.

Locking

Locking sessions and identities.

Teleport

How Teleport works



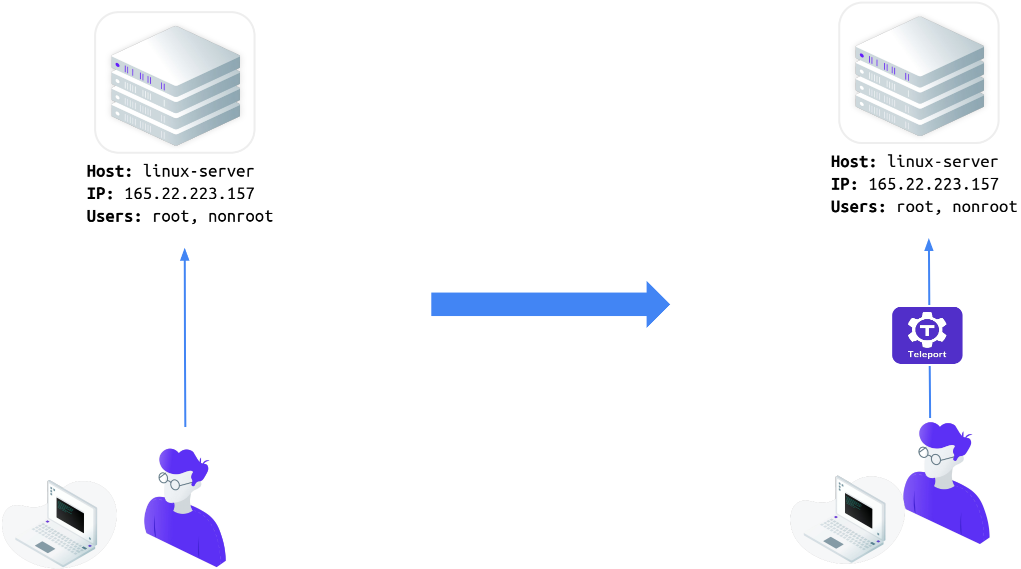
DEMO

Teleport

Demo 1

Teleport RBAC

Enforcing RBAC to SSH access using Teleport



Host: linux-server
IP: 165.22.223.157
Users: root, nonroot

Host: linux-server
IP: 165.22.223.157
Users: root, nonroot

Developer frequently accesses linux-server as a “root” user.

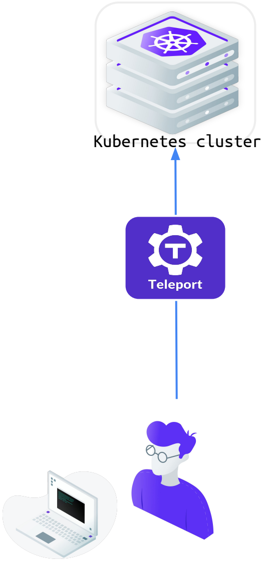
Developer will be required to access linux-server via teleport bastion and is authorized to connect only as a “nonroot” user account.

Teleport

Demo 2

Teleport Access Requests

Enforcing just in time privilege to Kubernetes Access



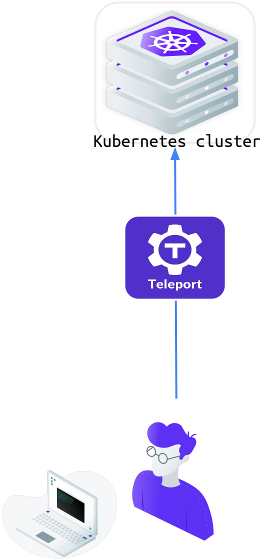
Contractor needs to access Kubernetes Cluster but is not assigned any Kubernetes privilege by default. To access the cluster, the contractor requires requesting role named “kube-member”.

Teleport

Demo 3

Teleport Session Locking

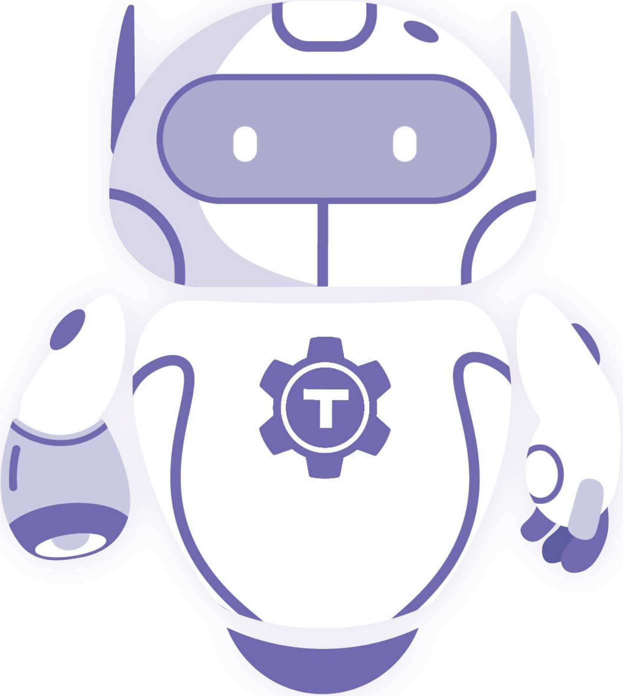
Enforcing session locking to lock out malicious user



Contractor session seems malicious. Contractors access will be locked for 50 minutes.

Teleport

Recommended Next Steps



Download Teleport

https://goteleport.com/teleport/download/

Read Teleport Access control docs

https://goteleport.com/docs/access-controls/introduction/

Check us out on Github

https://github.com/gravitational/teleport