Keeper Connection Manager vs Teleport: Feature Comparison

Keeper Connection Manager is the best Teleport alternative because it's easy to deploy on any device, unlike Teleport which has an extremely complex deployment model.

KEEPER	Teleport
Robust platform vs Stand-alone tool	
Keeper Security offers powerful connection management and Privileged Access Management (PAM) functionalities to thousands of enterprises and millions of users. These capabilities are seamlessly integrated into a highly secure enterprise password management and secrets management platform. Keeper Connection Manager, a remote access gateway, is fully integrated into the Keeper ecosystem, which protects organizations from password-related data breaches and cyberthreats.	**Teleport** is a stand-alone connection tool for software engineers that provides access to infrastructure through the use of short-lived certificates.
Installation	
Keeper Connection Manager is 100% agentless and clientless. No configuration or 3rd party services need to be installed on the target instances, and there is no risk of breach from third-party agents. Keeper Connection Manager only requires a simple Docker container to be installed in the target environment.	**Teleport** requires installation of agent software on every endpoint that will be accessed. In addition, it requires the installation of an Auth Server and a proxy server. Depending on what the users are accessing, organizations may also need to install clients like "tsh."
Encryption	
Keeper Connection Manager is both zero-knowledge and zero-trust. Keeper cannot access the infrastructure that is managed by the customer. When coupled with Keeper Secrets Manager for credential storage, Keeper provides zero-knowledge encryption of service account passwords and other access credentials.	**Teleport Cloud** is hosted by Gravitational and routes all connections through a centralized proxy. Unauthorized access to the Auth Server grants certificates that can log in to any managed host. Depending on the use case, the TLS session may be decrypted on the server.
Deployment model	
Keeper Connection Manager is easy to deploy on any device using a lightweight Docker container.	**Teleport's** deployment model is extremely complex and requires an agent, a central proxy and a central Auth Server. Additionally, per Teleport's own documentation, the solution utilizes features that are not considered "production-ready." Teleport software must be deployed on every instance.
Support for native RDP and SSH protocols	
Keeper Connection Manager uses standard RDP connections that do not require an admin to reconfigure the organization's entire data environment. The credentials used to access the destination server are managed by the admin and are never exposed to the end user. Session recordings are available for auditing purposes.	**Teleport** requires access to the domain controller for RDP access, a Linux instance, GPO changes, approval of a Teleport CA, and implementation of Smart Card APIs. This method of desktop access is extremely complex and works outside of the norm for the typical enterprise setup. Additionally, Teleport's RDP sessions cannot be recorded for auditing purposes.
Security model	
The **Keeper Connection Manager** gateway can be completely locked down to the customer's infrastructure to limit access between the client device and target server. Secrets that are used to connect to target servers can be managed within the Keeper Secrets Manager encrypted vault. Pass-through credentials also provide dynamic access to target instances for any user without storage of secrets anywhere in the gateway.	**Teleport Auth Server** issues short-lived credentials and is a single point of compromise. Compromise of the Teleport Auth Server would permit access to any node running the Teleport agent. This system also hosts a User CA -- this is a long-lived key, and exfiltration of this signing key permits an attacker to mint their own credentials to any Teleport-managed host. The Teleport architecture provides a much larger attack surface.
Monitoring, auditing and reporting options	
Keeper offers extensive reporting on privileged user behavior. In addition to providing aggregate security audits, Keeper also provides event logging for over 140 event types, event-based alerts and integration with popular third-party SIEM solutions. Keeper's compliance reporting functionality also allows admins to monitor and report access permissions of privileged accounts across the entire organization, in a zero-trust and zero-knowledge security environment.	**Teleport** has limited reporting and monitoring tools. It offers no password event data logging or robust compliance reporting functionality.
Organization and sharing capabilities	
In **Keeper Connection Manager's** model, end users have no access to the underlying credentials used to broker the connection. Keeper allows users to access systems the way they currently use them, with service accounts, local accounts, admin credentials or pass-through dynamic credentials.	**Teleport** requires the use of certificate-based authentication for desktop access, which involves modifying the way teams currently connect to targets and making configuration changes on the organization's domain controllers.
Secrets management	
Keeper Secrets Manager is a fully managed, cloud-based, zero-knowledge platform for securing infrastructure secrets such as API keys, database passwords, access keys, certificates and any type of confidential data – integrated directly into Keeper.	**Teleport** does not offer secrets management or encryption of digital assets.