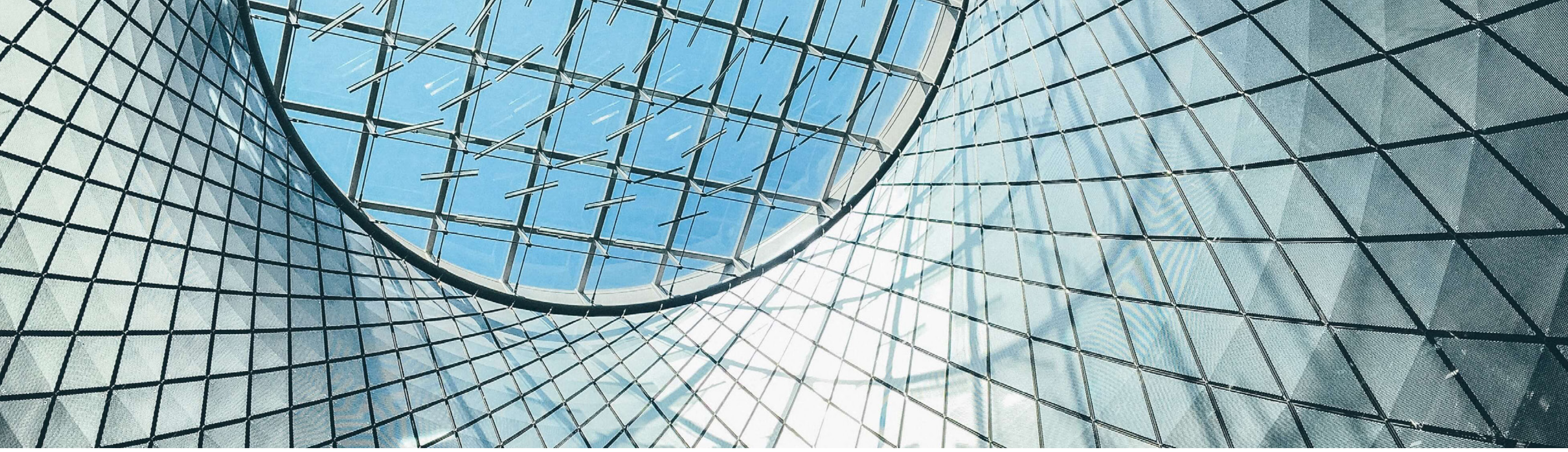


Market Insight Report Reprint

Coverage Initiation: Teleport 'shifts left' with cloud-native PAM platform

January 28 2022

by Garrett Bekker

'Shifting left' has become a thing in security circles, and addressing the needs of developers is no less true in the privileged access management market. Teleport's Access Plane combines connectivity, authentication, authorization and auditing functionality into a single PAM platform.

451 Research

S&P Global
Market Intelligence

Introduction

As we have outlined in a series of recent reports, ‘shifting-left’ has become a ‘thing’ in security circles, a phenomenon perhaps best highlighted by Okta’s $6.5bn purchase of developer-focused customer IAM (CIAM) provider Auth0. The requirement to address the needs of developers is equally true in the privileged access management (PAM) market, particularly as modern cloud-native architectures become more commonplace, as we outlined in our recent report on startup Akeyless. In addition to standard Linux and Windows servers, most firms now have heterogenous infrastructure to support, including containers running in Kubernetes clusters and traditional apps that have been ‘lifted and shifted’ to the cloud and now run in multicloud infrastructure environments.

Such firms may also have diverse sets of users that need various levels of access to this diverse infrastructure, including developers and cloud engineers that have their own apps and workflow tools like Jenkins or Jira. To address many of the various permutations of access scenarios, Teleport has come to market with what it calls the ‘Teleport Access Plane,’ which combines connectivity, authentication, authorization and auditing functionality into a single platform that could rightly be viewed as ‘Okta for infrastructure.’

THE TAKE

Many legacy PAM products were designed for managing on-premises infrastructure, but face challenges when dealing with cloud-native infrastructure and DevOps-driven processes. Teleport bills itself as the ‘easiest and most secure way to access heterogenous infrastructure.’ To the extent that it addresses those challenges, Teleport can be fairly described as ‘cloud-native PAM,’ and fits within recent efforts to deliver just-in-time PAM that eliminates the need for standing privileges and standard password vaults. Many of the latter rely on ‘shared secrets’ like SSH passwords that are shared among multiple people using admin accounts and must be rotated and managed throughout their lifecycle. By using short-lived identity-based certificates instead of static credentials like passwords, Teleport believes it offers a more secure way to provide privileged access that is more sustainable and allows for a smaller blast radius if compromised. The challenge will be to convert customers to a new way of thinking about PAM and fend off inevitable responses from legacy PAM vendors retooling or expanding their offerings.

Context

Teleport, originally Gravitational, was founded in 2015 as a developer-focused offering to deal with the problem of managing remote infrastructure. Rebranded as Teleport in 2020, the company now offers the Teleport Access Plane with both open source and commercial offerings. The company is led by CEO Ev Kontsevoy, who also founded Mailgun, a managed email provider that provided an API-based programmable email platform that enabled developers to add email to applications and which was sold to Rackspace in 2012. Teleport operates virtually, with an official HQ in Oakland, California, with about 160 full time employees and over 200 customers. Teleport has raised nearly $60m, most recently a series B round led by prior investor Kleiner Perkins, and plans to raise a series C round in the next two years.

Products

The Teleport Access Plane consists of four core components addressing connectivity (Teleport Connect), authentication (Teleport Authenticate), authorization (Teleport Authorize) and auditing (Teleport Audit) functionality in a single platform.

Teleport Connect is essentially a zero trust network access (ZTNA) product that allows users to connect to any resource in their global infrastructure regardless of network boundaries. Architecturally, unlike many PAM offerings that are based on a bastion host model, Teleport Connect functions as a 'multi-protocol, identity aware' access proxy that sits in front of an organization's infrastructure and proxies all connections to servers, databases and other supported resources via reverse tunnels protected with mutual TLS (mTLS). This allows customers to open only one network port for their entire infrastructure and maintain tight control over all access.

Teleport technically functions as a certificate authority (CA) that issues short-lived certificates to allow clients access to a firm's infrastructure. Teleport can be either cloud or self-hosted, and the cloud version reroutes traffic to the lowest latency routes to maintain performance requirements. Like other offerings that employ a CA, Teleport also recommends that customers use hardware security modules (HSMs) to protect the CA.

Teleport Authentication provides identity-based authentication for humans, machines and services – Jenkins bots as well as 'Johnny the network admin' – to access resources (servers, databases, Kubernetes clusters, DevOps tooling like CICD, version control, monitoring and metrics dashboards, etc.). Teleport offers single sign-on (SSO) integration with standard identity providers (IdPs) such as Active Directory (AD), Azure AD or Okta, from which it can pull role data and issue short-lived mTLS certificates that are used for accessing any infrastructure resource.

Teleport Authorize ingests the role data from the IdP to perform fine-grained, role-based access controls (RBAC) for employees and services. Authorize also offers access request workflows for more granular authorization processes. For example, a developer who needs access to a production resource, but is prohibited by a least privilege (LP) policy, could be granted an exception in an agile way to get access to resources through chat ops (integration between Teleport and Slack, Jira, Mattermost or other systems) and dual authorization and session moderation (having a second person to monitor actions as they are accessing a production resource such as a server or database).

The Teleport Access Plane platform is composed of five products that provide specific capabilities for different types of infrastructure that have unique requirements, or what it calls 'protocols.' These protocols are supported by the following Teleport products: SSH (Teleport Server Access), Windows RDP (Teleport Desktop Access), Kubernetes (Teleport Kubernetes Access), MySQL, PostgreSQL, and MongoDB (Teleport Database Access), Internal DevOps applications (Teleport Application Access). Each component of the Teleport Access Plane (connectivity, authentication, authorization and audit) can be applied at the protocol level for each piece of infrastructure.

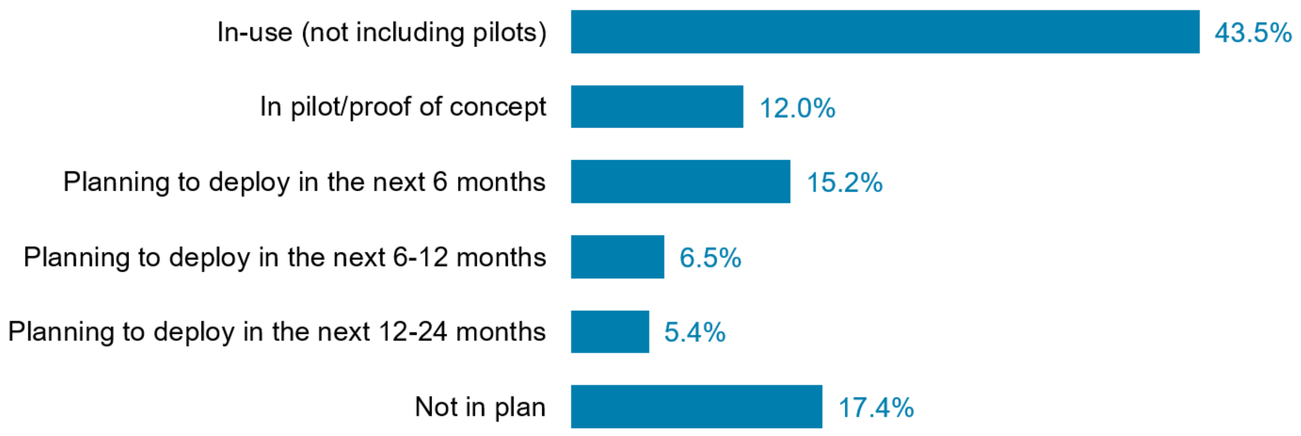
Teleport Audit provides visibility into infrastructure access and behavior to help meet compliance objectives (such as NIST, SOC2, FedRAMP). Audit also provides session recordings, live views of all active sessions, detailed change logs and can integrate with existing SIEM tools.

Strategy

In terms of customers, Teleport targets organizations that need to demonstrate security and compliance for their infrastructure to comply with mandates such as SOC 2 and FedRAMP, but who also operate in high-growth industries where agility is required, including SaaS companies, crypto exchanges, fintech and financial services companies, large-scale gaming and entertainment companies, and newly public tech companies, many of which are DevOps-centric. Companies looking to do 'modern' PAM in a DevOps environment are also target customers.

Common personas for Teleport customers include security-minded engineers, specifically DevOps engineers who may need, for example, to log into a Jenkins cluster to deploy new apps into production, or a site reliability engineer who may need to log into a production database after requesting elevated access using a just-in-time request via a ChatOps or PagerDuty system. Teleport appeals to engineers who are unable to meet the security and compliance standards required to pass third-party audits or are dissatisfied with existing PAM approaches that were not designed for cloud-native environments. While the current go-to-market plan is very engineer-driven, the longer-term growth plan will target the C-suite and above by focusing on more strategic rather than tactical messaging. The challenge will be to balance the needs of both groups by courting executives and senior management without alienating their core champions in DevOps and engineering.

Forty-four Percent (44%) Of Firms Have Already Deployed PAM; 27% Plan To Deploy With 24 Months



Q. What is your organization's status of implementation for the following information security technologies?

- Privileged access management (PAM)

Base: All respondents (n=92)

Source: 451 Research, Voice of the Enterprise: Information Security, Workloads & Key Projects 2021

Competition

Teleport's most direct competitors are likely traditional PAM vendors, such as BeyondTrust, Broadcom (CA/Xceedium), Centrify, CyberArk, One Identity and Thycotic, as well as Manage Engine and Wallix. Newer PAM vendors with a greater focus on JIT privileged access include Remediant, STEALTHbits Technologies (acquired by Netwrix) and Xton (acquired by Imprivata). However, Teleport may be most directly competitive with vendors that offer PAM capabilities with a focus on DevOps, including HashiCorp, Akeyless, Iraje, Senhasagura and the midmarket-focused StrongDM. HashiCorp's Vault is capable of doing 'traditional' secrets management, while Consul also provides a distributed key store in contrast to Teleport's reliance on short-lived certificates.

Although Teleport Connect has ZTNA functionality, the company is not competing directly with ZTNA vendors looking to provide remote access for entire workforces. The list of ZTNA vendors is long, and includes Appgate, Banyan Ops, Netskope, Palo Alto Networks, Perimeter 81, Check Point Software (via the acquisition of Odo Security), Fortinet (OPAQ Networks), Cisco, Juniper Networks, VMware, Google, Microsoft, Proofpoint (Meta Networks), Zscaler, Forcepoint, Ivanti (PulseSecure), Akamai (Soha Systems), Cloudflare, Broadcom (Luminate Security), Verizon (Vidder) and Barracuda.

SWOT Analysis

STRENGTHS

Teleport combines connectivity, authentication, authorization and audit capabilities in a single 'cloud-native PAM' offering. Certificate-based architecture can allow for more granular, nuanced role-based access control that can limit attack surface. It can integrate into modern DevOps workflows.

WEAKNESSES

As a CA, customers may want to use HSMs to protect Teleport's bastion host, which essentially contains the 'keys to the kingdom.' Teleport will also need to balance the needs of executives and senior management without alienating its champions in DevOps and engineering.

OPPORTUNITIES

Target customers include organizations that need audit results for compliance mandates and want to self-regulate, as well as companies looking to do 'modern' PAM in a DevOps environment. Use of short-lived certificates could also allow Teleport to target traditional PAM opportunities as an alternative to password vaults.

THREATS

Teleport's challenge will be to convert customers to a new way of thinking about PAM, as well as fend off inevitable responses from legacy PAM vendors retooling or expanding their offerings.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.