TAG

SPECIAL ANALYST REPORT

TOP FIVE DATA ACCESS GOVERNANCE VENDORS

2025

Teleport

SPECIAL ANALYST REPORT

TOP FIVE DATA ACCESS GOVERNANCE VENDORS – 2025

PREPARED BY THE TAG ANALYST TEAM

www.tag-infosphere.com

LEAD ANALYST: DR. EDWARD AMOROSO

Chief Executive Officer, TAG Infosphere[1]

Research Professor, NYU[2]

eamoroso@tag-cyber.com

Version 1.0
2025

This TAG Analyst Report features the TAG Top Five vendor Teleport in the area of Data Access Governance for 2025 based on TAG's evaluation criteria..

Teleport provides DAG capabilities by securing access to infrastructure for developers and infrastructure teams, focusing on identity-based access management. By unifying trusted identity, zero trust authentication, and ephemeral authorization with role-based and attribute-based access control, Teleport ensures that only authorized users can access sensitive systems and data. Additionally, Teleport's session recording, auditing, and identity governance features provide organizations with visibility into user activity, making it easier to detect and respond to unauthorized access attempts. This combination of secure access management and auditing aligns with DAG principles, helping companies safeguard data and meet compliance requirements.

INTRODUCTION

Data Access Governance (DAG) is an essential component of modern data security strategies, focusing on managing and controlling access to sensitive data across an organization. As businesses accumulate massive amounts of data, the challenge of ensuring that only the right people have access to specific data sets becomes critical. DAG helps organizations enforce policies around who can access what data, under what conditions, and for what purpose.

A core function of DAG is data access visibility, which provides insights into where sensitive data resides and who currently has access to it. This visibility enables security and compliance teams to understand the data access landscape and make decisions about access permissions. By continuously monitoring data access patterns, organizations can detect and flag unusual access requests, such as unauthorized users attempting to view restricted information.

DAG also plays a critical role in managing access based on least privilege. By ensuring that employees have only the minimum level of access required to perform their jobs, DAG helps limit exposure in the event of a data breach or insider threat. Implementing least-privilege access controls across an organization can be challenging, especially in large environments with complex permissions. DAG solutions automate the process of analyzing roles and permissions, helping organizations align access controls with business needs while minimizing risk.

Another key aspect of DAG is entitlement management, which involves defining, managing, and periodically reviewing access rights. Entitlement management allows organizations to maintain an understanding of who has access to specific data sets and why, ensuring that access permissions are not overly broad or outdated. By establishing automated workflows for approving, revoking, and auditing data access rights, DAG solutions streamline the governance process and ensure that permissions remain current. Regular access reviews are also critical for identifying security gaps, especially as employees change roles or leave the organization.

Finally, DAG supports data access policy enforcement and compliance. Many organizations operate in highly regulated industries where data privacy and security regulations require them to document and enforce access policies. DAG solutions provide tools to create and enforce granular access policies, ensuring that users adhere to established security protocols.

EVALUATION CRITERIA

The process for calculating a TAG Navigator to determine the aggregate CVR for a cybersecurity vendor involves ten factors. How these factors are used has evolved and is now associated with a common, normalized interpretation and scoring that is being used in various sectors including cyber insurance as a basis for reviewing the effectiveness of a vendor in reducing the cyber risk of buyers. The ten factors are as follows:

1. **Company Stage:** This references where a given vendor currently resides in the corporate lifecycle. At one end of the scale are the start-ups driven by founding teams. Mature public companies with experienced management are at the other end of the scale.

2. **Message Efficacy:** This involves the vendor's marketing and value proposition message. At one end of the spectrum is an unclear description focused mostly on features. At the other end is a strong message of what solution is being addressed and why.

3. Pace of Innovation: This involves how rapidly the vendor is innovating. At one end of the scale are the vendors innovating at an impressive pace. At the other end of the scale are companies who slow innovation in favor of scale.

4. Vision and Strategy: This addresses whether the vendor articulates their role and purpose. At one end of the scale are vendors developing a future vision. At the other end of the scale are vendors who describe a clear vision and strategy for their company.

5. Strength of Management: This references whether a strong management team exists. At one end of the spectrum are companies with new managers in their first leadership roles. At the other end are companies with a mature, experienced leadership team.

6. Strength of References: This involves the references who can vouch for a vendor. At one end of the scale are new vendors with virtually zero customers and at the other end, we find vendors with massive global customer bases.

7. Financial Strength: This addresses the company's funding, revenue, and profitability. At one end of the spectrum are companies with weak near-term financial prospects. At the other end are well-funded or public companies with growing revenue and profits.

8. Ability to Scale: This addresses whether the solution can be provided to a large base. At one end of the spectrum are companies that struggle to support new customers. At the other end are companies with a platform that can handle rapid growth.

9. Product Functionality: This references whether the solution addresses the needs of its customers. At one end of the spectrum are companies with a prototype. At the other end are companies with a working solution that is thoroughly used and supported.

10. Infrastructure Maturity: This references whether the company is sufficiently protecting user data and ensuring proper support for customer security. New vendors are usually challenged in this area and often do not have security teams in place.

More information on these ten factors that comprise the set of criteria used in rating cybersecurity vendors is available on-demand from TAG. Research as a Service (RaaS) customers can review the justifications for ratings through their TAG RaaS portal account. They can also obtain more detailed guidance on roughly 4700 commercial cybersecurity vendors. Information on TAG RaaS subscriptions can be obtained at https://www.tag-infosphere.com/.

DATA ACCESS GOVERNANCE
TOP-TIER VENDOR PROFILE

TELEPORT

CVR RATING
8.1
(scale 0 to 10)
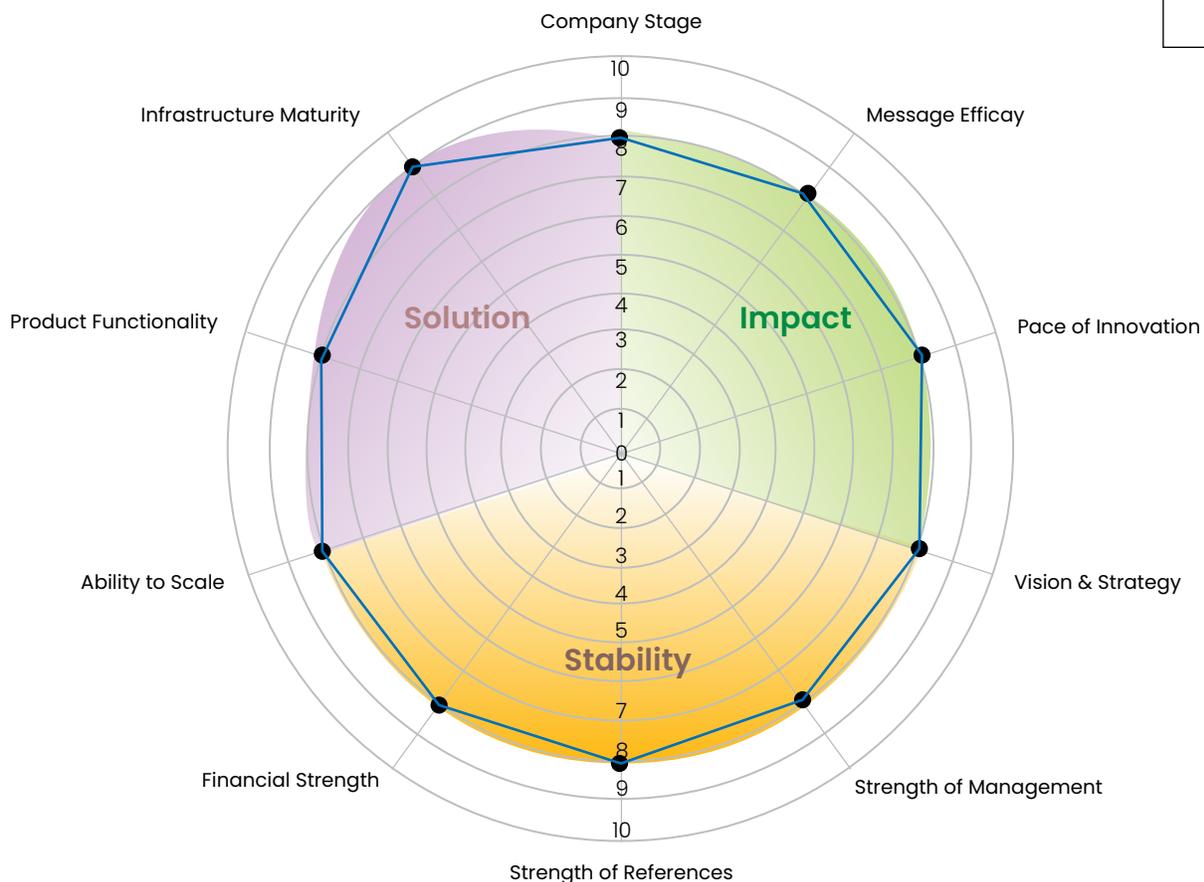
Teleport supports Data Access Governance for enterprises by providing a unified access platform that secures and monitors access to critical infrastructure, applications, and data. With its focus on Zero Trust security principles, Teleport ensures that users only have access to resources necessary for their role, thereby limiting the risk of unauthorized access.

The platform offers robust session monitoring and recording capabilities, allowing organizations to track user activity in real time. Teleport enables enterprises to detect anomalies in access patterns, investigate potential threats, and address security incidents before they escalate. By integrating with various identity providers and offering multi-factor authentication, Teleport enhances security by ensuring that only verified, authorized users have access to enterprise data and resources.

Teleport also simplifies compliance with industry regulations, such as FedRAMP, HIPAA, and SOC 2, by automating access logs and maintaining detailed audit trails. These records allow enterprises to demonstrate adherence to data access requirements, aiding in regulatory audits and reducing the risk of compliance penalties.

Methodology: The TAG Navigator uses 10 factors to assess vendor's solutions. Each factor represents a key aspect of the solution's value and has been deemed by TAG as a reasonable predictor of its success in the discipline. TAG's Cyber Vendor Ratings (CVR) factors are rated on a scale of 1-10. The solution analyzed above has been selected by TAG as a top-tier solution within the discipline.

TAG

SPECIAL ANALYST REPORT

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to provide on demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science.

tag-infosphere.com

⚙ Teleport

ABOUT TELEPORT

Trusted by the world's most innovative companies, Teleport is the Infrastructure Identity Company, modernizing identity, access, and policy for infrastructure, improving engineering velocity and resiliency of critical infrastructure against human factors and/or compromise.

goteleport.com