britive

Teleport secures infrastructure identity. **Britive unifies every layer of access.**

Teleport is a strong infrastructure identity platform. It gives engineers cryptographic, audited access to servers, databases, Kubernetes clusters, and applications — replacing shared secrets with short-lived certificates. For teams hardening how people connect to infrastructure, Teleport delivers a sophisticated experience.

Its architecture also defines its scope. Teleport sits in the data path between users and resources, which means the surfaces it governs are the surfaces it can connect to. Cloud IAM, SaaS administrative permissions, and continuous policy enforcement across the broader access layer fall outside what an infrastructure proxy is built to address.

Britive operates at the entitlement layer instead of the connection layer. Without sitting in the data path, Britive provisions and revokes access directly across cloud IAM, SaaS, on-prem, machine identities, and AI agents — all under one policy engine.

Teleport secures infrastructure identity. Britive governs every layer of access.

WHAT SETS BRITIVE APART

- No cluster. No proxy. No data path dependency. Britive provisions access at the entitlement layer via native cloud APIs, nothing to deploy, scale, or maintain in your environment.
- Direct cloud IAM and SaaS permission governance, not just federation. Britive provisions and revokes AWS IAM, Azure RBAC, GCP, and SaaS admin permissions at the control plane.
- Continuous policy enforcement, not point-in-time checks. Evaluation happens continuously to respond dynamically to changes to risk posture.

Teleport vs Britive

TWO ARCHITECTURES FOR TWO DIFFERENT LAYERS OF ACCESS

	TELEPORT	BRITIVE
Architecture	Cluster + proxy + agent model. Users connect through the Teleport proxy; resources register with the cluster via an installed agent. Teleport sits in the data path.	Control-plane native. Britive provisions access via native cloud APIs and exits the data path. No cluster, proxy, or agents deployed in customer environments.
Infrastructure Access	Cryptographic, certificate-based access to servers (SSH/RDP), databases, Kubernetes clusters, Windows desktops, and applications, with built-in session recording and audit.	Strong via Access Broker. Proxyless JIT access to databases, Kubernetes, and servers across cloud and on-prem environments without sitting in the data path.
Cloud IAM	AWS Console, CLI, and API access via OIDC federation or IAM Roles Anywhere. Users assume existing IAM roles routed through Teleport.	Native JIT for AWS IAM, Azure RBAC, GCP bindings, and OCI. Access provisioned and revoked directly at the control plane, not federated through a proxy.
SaaS Coverage	Application access via SSO and reverse proxy for SAML/OIDC apps. No native administrative governance for SaaS platforms.	Native JIT with deeper administrative governance for Snowflake, Salesforce, ServiceNow, Atlassian, GitHub, and 100+ more under one policy model.
Agentic AI Identities	Beams (launched 2026) provides isolated Firecracker VM runtimes for AI agents with identity-bound access and no static secrets.	Distinct identity class governed by an MCP Gateway and agent registry. Human-in-the-loop approval and SPIFFE federation enforced at request time, with full audit trail.
Non-Human Identities	Machine & Workload Identity issues short-lived X.509 and SPIFFE-format certificates via the tbot agent. Strong cryptographic NHI model bound to infrastructure resources.	First-class NHI governance with OIDC/SPIFFE federation, JIT per pipeline run, and a full registry for lifecycle management, without an agent deployed in customer environments.
Device Posture & Enforcement	Device posture verified at access request. Identity locking instantly revokes access across infrastructure when a user is compromised. Point-in-time enforcement.	SSF/CAEP allow for continuous enforcement. Sessions terminate the moment device, location, or context signals change mid-flight.
Developer Workflow	Native experience via the tsh CLI, Web UI, and IDE integrations. Approval workflows via Slack, PagerDuty, Teams, Jira, and ServiceNow.	Native experience via PyBritive CLI, Terraform provider, browser extension, and ChatOps. IaC-first with support for policy-as-code.