britive

CyberArk manages standing credentials. **Britive eliminates them.**

CyberArk built the standard for enterprise privileged access management. But whether deployed on-premises or hosted as a SaaS platform (Privilege Cloud), their core architecture remains the same: it is designed to store, rotate, and proxy standing credentials.

Cloud infrastructure works differently. AWS IAM roles, Azure RBAC assignments, and GCP project bindings are dynamic entitlements, not static accounts. They don't have passwords to vault. Furthermore, with non-human identities and automated pipelines outnumbering humans 40:1, or up to 100:1 in cloud DevOps heavy environments, a credential-centric vault model creates severe operational bottlenecks.

Britive governs the cloud IAM, SaaS, and machine identity layer from the ground up—without relying on vaults, heavy session proxies, or standing credentials. Access is provisioned via native API at the moment of request, scoped to exactly what the task requires, and auto-revoked on completion. Nothing exists before the request. Nothing remains after.

CyberArk protects the credential. Britive eliminates the need for one to persist.

WHAT SETS BRITIVE APART

- Britive mints time-bound permissions at request time via native cloud APIs—leaving zero standing access. CyberArk's core JIT relies on checking out a vaulted account for a session window. Even with their newer cloud modules, the underlying architecture heavily relies on standing access and static secrets.
- Britive is an API-first platform. No per-endpoint licensing and no heavy infrastructure to maintain. CyberArk's cloud deployment still requires managing complex network connectors and routing developers through heavy session proxies that break cloud velocity.
- Britive deploys natively across your cloud environments in weeks as a single, unified policy engine. To achieve similar multi-cloud and machine identity coverage with CyberArk, organizations must stitch together multiple disparate products, requiring higher integration overhead and professional services.

CyberArk vs Britive

THE ARCHITECTURAL DIFFERENCE, SIDE BY SIDE

	CYBERARK	BRITIVE
Architecture	Even in SaaS form, the core engine relies on storing static secrets in a vault and routing sessions through heavy proxies.	Permissions are provisioned at runtime time via native cloud APIs and revoked automatically. No vaults or proxies required.
Cloud IAM	Cloud access is handled by a separate module added onto the vault foundation, resulting in potentially fragmented policies.	Complete entitlement visibility and JIT access enforcement natively built into a single policy engine across AWS, Azure, GCP, and OCI.
Deployment & Time to Value	18–36 months for enterprise. High professional services overhead required to configure required network connectors, session managers, and modules.	Weeks for cloud environments using native APIs. No professional services for standard cloud use cases.
Non-Human Identities	Credential-centric model for service accounts with vaulting and rotation of static secrets for workloads.	First-class NHI governance. OIDC workload federation, JIT per pipeline run.
Agentic AI	Lacks architectural governance for dynamic MCP connections and relies heavily on standard machine credentials.	Distinct identity class governed by an MCP Gateway and agent registry. Access minted strictly for AI's task duration with full audit trail.
SaaS Coverage	Primarily manages SaaS access by vaulting shared administrative credentials or relying on basic SSO step-ups.	Grants dynamic, auto-revoking access for Snowflake, Salesforce, Atlassian, ServiceNow, GitHub, and 100+ applications.
Developer Adoption	Forcing developers to break their native flow to route through a web portal or session proxy often leads to bypassed security controls.	Integrates seamlessly via PyBritive CLI and Terraform provider. Security is invisible; developers stay in their native workflows.
Vendor Risk	Post-acquisition integration. Product roadmaps and engineering focus are diverted toward cross-platform consolidation rather than cloud-native innovation.	Agile & analyst validated. The only PAM provider chosen for AWS Security Hub Extended customers, proving the architectural depth required for a hybrid organization.