britive

# StrongDM governs the connection. **Britive governs the entitlement itself.**

StrongDM is a technically strong infrastructure access proxy that's developer-friendly, with solid session recording, clean approval workflows, and CrowdStrike device posture checks at request time. For governing access to databases, servers, and Kubernetes clusters, it delivers a good experience. The proxy architecture is also its structural constraint: StrongDM sits in the data path and reaches only resources that have a connector in front of them.

Cloud IAM roles, Azure RBAC assignments, GCP bindings, SaaS permissions, and CI/CD pipeline credentials live above the connection layer, all outside what a proxy can govern.

Britive provisions ephemeral access at the entitlement layer via native cloud APIs, then exits the data path. Cloud IAM, SaaS, NHI workloads, and AI agents are all governed under one policy engine. Nothing exists before the request. Nothing remains after.

StrongDM governs the connection. Britive governs the entitlement.

WHAT SETS BRITIVE APART

- No proxy. No data path dependency. Britive provisions access via native cloud APIs and exits the connection. There's no chokepoint to scale, harden, or route around.
- One policy engine across the entitlement layer. Cloud IAM, SaaS, NHI workloads, and AI agents are all governed under a single model, not through separate connectors or products per environment.
- Continuous enforcement, not point-in-time posture. Britive's dynamic authorization management and integration with the Shared Signals Framework (SSF) means that shifting device risk posture prompts action immediately.

## StrongDM vs Britive

TWO ARCHITECTURES FOR TWO DIFFERENT LAYERS OF ACCESS

| | STRONGDM | BRITIVE |
|---|---|---|
| **Architecture** | Proxy model. Traffic flows through StrongDM gateways and relays, creating a data path dependency for every governed connection. | Control plane model. Britive provisions access via native APIs and exits the data path. No per-connection dependency. |
| **Infrastructure Access** | Strong. Managed proxy connections to databases, SSH/RDP servers, and Kubernetes clusters, with native session recording. | Strong via Access Broker. On-prem and infrastructure access without sitting in the data path or requiring proxy clusters. |
| **Cloud IAM** | Outside the proxy's reach. AWS IAM roles, Azure RBAC, GCP bindings, and OCI entitlements aren't governed at the connection layer. | Native JIT for AWS IAM, Azure RBAC, GCP bindings, and OCI — equal depth across all major clouds. |
| **SaaS Coverage** | Not natively addressed. The proxy model doesn't extend to SaaS permission governance. | Native JIT for Snowflake, Salesforce, ServiceNow, Atlassian, GitHub, and 100+ more under one policy model. |
| **Agentic AI Identities** | Not addressed at the architectural level. No MCP governance, agent registry, or human-in-the-loop controls. | Distinct identity class. MCP Gateway, agent registry, human-in-the-loop approval, and a full audit trail. |
| **Non-Human Identities** | Limited support for pipeline credentials. No full NHI lifecycle management or registry. | First-class NHI governance. OIDC federation, JIT per pipeline run, and full lifecycle management. |
| **Device Posture & Enforcement** | Device posture evaluated at the moment of access request. Point-in-time enforcement. | SSF/CAEP continuous enforcement. A non-compliant device mid-session terminates access immediately. |
| **Vendor Enforcement** | Acquired by Delinea in early 2025. Buyers should evaluate the integration timeline and product cohesion plan, given Delinea's prior consolidations. | Independent, with a single product line focused on cloud-native PAM. Selected as AWS's sole PAM partner for AWS Security Hub Extended. |