Bring Your Customers the PAM Model built for What's Next

Enterprises know they need privileged access management. Unfortunately, traditional, vault-dependent PAM has not kept pace with the requirements of the modern enterprise.

Modern environments demand more speed, stronger security, and a far more diverse privilege model across a wide technical landscape — cloud, SaaS, pipelines, and more.

About Britive

Britive takes a fundamentally different approach to privileged access management. Rather than relying on standing access and gated credentials, Britive focuses on true just-in-time, zero-standing privileges.

Standing access is the prime vector for many breaches. Britive solves that by removing access when it isn't actively being used by an authorized identity, minting privilege at runtime and destroying it when the work ends. This differs fundamentally from traditional toolsets, which preserve standing access and only gate access to the credentials.

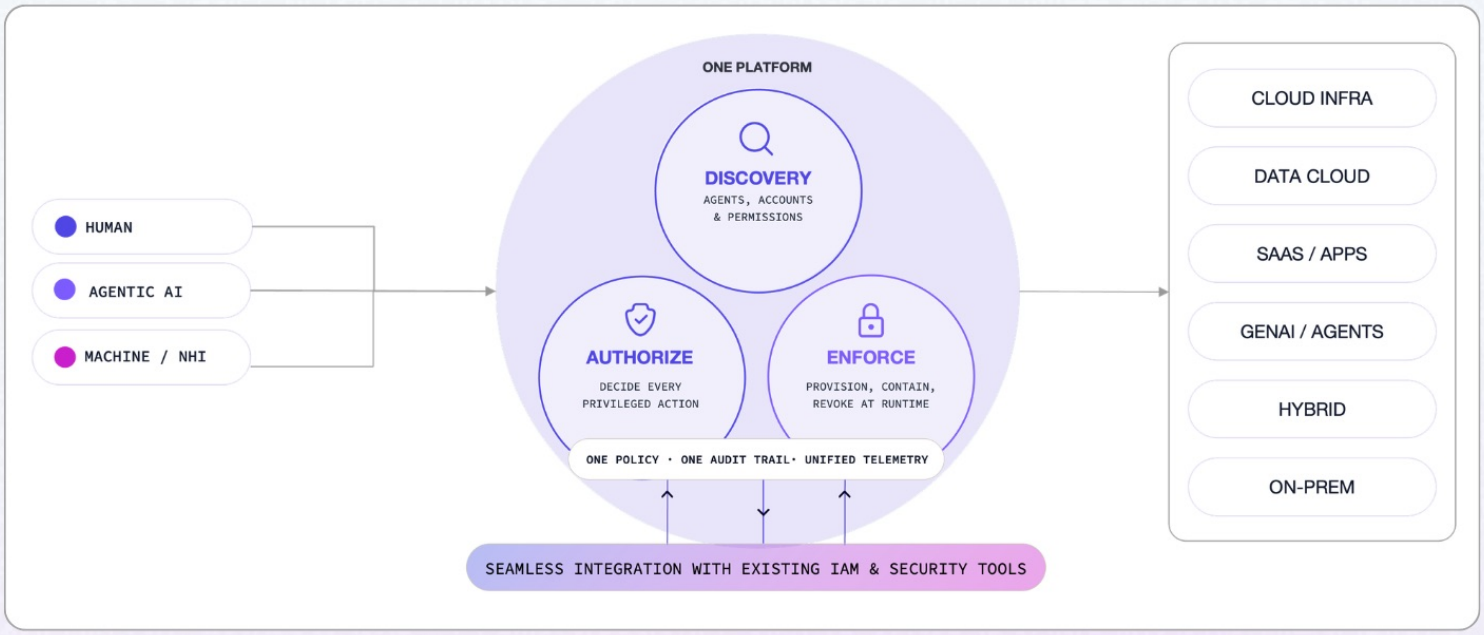
What Britive Does

How It Works

When an identity, human, AI agent, or machine needs access to a resource, Britive evaluates the identity in the context of its request.

If policy allows it, Britive creates a precisely scoped privilege on the target resource. When the work ends, the privilege is destroyed.

No access is provisioned in advance, and no access remains after a task is complete, so there is nothing left to steal, rotate, or clean up.



CAPABILITY	WHAT IT MEANS	WHY IT MATTERS
Context-aware runtime decisioning	Access is evaluated and granted at the moment of action, not assigned ahead of time, and can adapt or revoke mid-session on risk signals.	Access reflects current reality, not yesterday's assumptions.
True JIT — the permission, not access to a standing one	Britive creates the privilege for the action and removes it after; no privilege sits behind the grant.	Nothing standing to steal, reuse, or clean up.
One model across human, agentic AI, and machine identities	The same runtime decision governs every identity type — not a separate tool per type.	No gaps in the seams; nothing new to buy as identity types grow.
One model across cloud, hybrid, and on-prem	The same enforcement runs everywhere and reaches servers and databases, because it belongs to no single cloud.	One place to control access; no per-platform tool to staff.
AI agents as first-class identities	Registered, owned, given ephemeral on-behalf-of access, with human-in-the-loop for high-risk actions and policy-governed tool access.	Agent sprawl governed from day one, not found at audit.

The Results

Security delivered rapidly & scalably across your entire footprint.

Unify access for every identity and every environment under a single tool. Eliminate the duplicate costs, the gaps between point solutions, and the user friction caused by implementing multiple tools.

Improved security posture across the entire estate.

True zero standing access spans every identity type and every resource, whether in the cloud, SaaS, on-prem, or hybrid environments. Defend every part of your environment with a single tool.

Significantly lower total cost of ownership.

Secure your environment without endpoint agents or proxies for ephemeral access provisioning at runtime. Less infrastructure to maintain, fewer people required to manage and maintain secure access.

Security that operates at machine speed.

AI agents act faster than any human approval process can keep up with. Britive authorizes through policy, in the moment, so access keeps pace with how agents work instead of becoming what they wait on, while AI and cloud initiatives continue to move without security gating them.

Use Cases and Solutions

Extending privileged access to the cloud.	Being truly cloud-ready takes two things, and Britive is built for both: supporting the complex entitlement structures cloud services use across infrastructure-as-a-service and complex SaaS, and delivering the low-friction, fast, native-to-their-tooling experience that cloud and DevOps users have come to expect. This improves adoption in a way that vault-based PAM strategies cannot.
Full standing access elimination everywhere.	With no standing access anywhere, the result is a far more secure posture across the entire estate: cloud, SaaS, on-prem systems, databases, and DevOps pipelines alike. Privilege is created at runtime and removed when the work ends, so there is nothing standing to clean up after the fact.
Agentic AI and machine identity security.	Always-on access is the wrong model for autonomous identities, and their dynamic, machine-speed nature is what traditional PAM was never built to govern. Britive extends the same runtime model to non-human and agent identities, with no separate tool per type.
Regulatory compliance requirements.	Since privilege is created at runtime and nothing persists between sessions, requirements around least privilege, standing access, and audit evidence are met structurally, rather than with minimal compensating controls layered on top.

Customer Proof

Stats and testimonials from leaders across industries.

Various named, individual case studies available upon request.

A global investment firm:

"Britive gave us more coverage, more users, and a path to Zero Standing Privileges — for less."

~50%

per-user cost savings, allowing for scale across additional users

55%+

reduction in total cost of ownership vs previous vault-dependent PAM renewal cost

100%

privileged access coverage across multi-cloud environments across customer deployments

RELTIO BEHAVOX TOYOTA Forbes fiserv. firstmac Janus Henderson INVESTORS Veterans United Home Loans

Frequently Asked Questions

“Isn’t this just another vault or PAM?”

↳ A vault’s job is to store and broker standing credentials. Britive does not keep that store as the default — privilege is created at the moment of work and removed after, so there is nothing waiting in a vault to check out.

“I already have a JIT solution.”

↳ Most “JIT” time-boxes access to a privilege that permanently exists — a standing role rented for an hour. Britive creates the permission itself for the moment and destroys it after, so there is no standing role or account behind the grant. JIT access versus JIT permissions is the difference.

“Is this cloud-only?”

↳ No. The same runtime model runs across cloud, hybrid, and on-prem, reaches traditional resources like servers and databases, and applies the same way to human, agentic AI, and machine identities.

“Does removing standing access slow my teams down?”

↳ The opposite — access is requested and approved inside the tools teams already use: web UI, CLI, API, Terraform, Slack, Teams, CI/CD, a browser plugin, and MCP-native agent paths, with no ticket queue. The secure path becomes the fast path, so people stop routing around it.

“Can Britive integrate with _____?”

↳ Britive is API-first, with 100+ integrations available out of the box across cloud infrastructure, applications, and data; others are established via API or, in many cases, no-code configuration.

“What do we actually have to deploy?”

↳ Less than vault-, proxy-, or endpoint-dependent PAM. For cloud and SaaS use cases there is nothing to deploy — Britive is agentless and proxyless, with no connectors to host. The access plane is proxyless; an audit-plane bridge activates only for targeted session recording where policy requires it.

“What happens if Britive has an outage — is there break-glass access?”

↳ Britive runs on a highly available, cloud-native architecture, with emergency access procedures for when the normal path is unavailable.

“Beyond the software, where are the services opportunities?”

↳ Moving a customer to runtime is a journey that can benefit from multiple partner services: discovering and cleaning up standing accounts; integrating Britive across the customer’s identity stack; enabling and re-educating users to adopt just-in-time; re-architecting applications that have static credentials built in; and re-evaluating DevOps pipelines to remove standing access. The software lands the deal; the customer journey is where the ongoing services revenue is.

Next Steps

Reach out for a deep dive to see the technology in action.

Book a product walkthrough