

>_ CUSTOMER CASE STUDY

From Static PAM to One Runtime Access: 55%+ Cost Savings Securing Human & Non-Human Identities

Global investment manager replaces credential-centric PAM with Britive, deploying across a complex hybrid environment in weeks, cutting projected PAM spend more than 55%, closing the NHI and human identity security gap, and building the runtime foundation for agentic AI adoption.

~55%+

55%+ Reduction in TCO
License savings only.
Total savings higher.

2x

More users covered
at a lower total cost

4x

More environments
from zero cloud coverage
→ four platforms

50%

per-user cost savings,
able to scale to more
users for less

"The renewal quote from our previous vendor was the forcing function. When we saw what it would cost to properly deploy what we already had, the decision became straightforward. Britive gave us more coverage, more users, and a path to Zero Standing Privileges — for less."

— GLOBAL HEAD OF IAM

ABOUT THE
INVESTMENT
FIRM INVESTORS

This customer is a global active asset management firm managing hundreds of billions in assets, operating across North America, Europe, and Asia Pacific. Their technology infrastructure spans a complex hybrid environment: three separate Active Directory forests, Azure, Snowflake, Databricks, AWS, Salesforce, and GitHub, with a significant on-premises footprint managed alongside a growing cloud presence.

[01] THE CHALLENGES

Like many organizations with roots in on-premises infrastructure, the customer’s privileged access management had evolved around a vault-based model. Their existing PAM tool, Secret Server, vaulted and rotated passwords for on-premises accounts. That was largely the extent of its reach. Two structural gaps had been growing in parallel: the environment had shifted toward cloud platforms the tool could not reach, and hundreds of non-human identities, service accounts running across Active Directory, Oracle DB, and network infrastructure, were operating outside any runtime enforcement model entirely.

As the environment shifted toward the cloud, the gaps became harder to ignore.

No cloud coverage	Their existing PAM tool had no meaningful integration with Azure. It couldn't touch Snowflake, Databricks, or GitHub. A core use case: service accounts storing credentials in Azure Entra Key Vault. That was something the existing tool explicitly could not support. The team had been evaluating Azure PIM as a stopgap. The goal was a single platform for both cloud and on-premises access.
Non-human identities operating without runtime controls	This is one of the most significant NHI security challenges in the deployment, and one of the most common in enterprise environments: machine identities running on static credentials with no runtime enforcement, no automatic revocation, and no meaningful audit trail. Global Head of IAM, described the situation plainly. Hundreds, possibly thousands, of non-human identities, service accounts spanning Active Directory, Oracle DB, and network infrastructure, were operating with no visibility into whether they were active, who owned them, or what they had access to. No standing access was being challenged. No credential was expiring on its own. The prior PAM tool's discovery capabilities returned nothing actionable, and the team had resorted to using a third-party SIEM just to track service account activity. The NHI security gap was not a configuration problem. It was an architectural one: a static credential model applied to identities that required runtime controls
Standing access that nobody could justify	The vault-based architecture meant that access persisted indefinitely. Human users and non-human identities alike held standing permissions to systems whether they needed them in that moment or not. Secrets were vaulted in folders visible across teams. Users could see each other’s access. There was no just-in-time model, no ephemeral access, no automatic expiration. For non-human identities specifically, this meant service account credentials remained active and accessible around the clock, whether a workload was running or not. When any account was compromised, the blast radius was whatever that identity had standing access to. For a service account with broad infrastructure access, that blast radius was significant.
A tool barely deployed despite years of ownership	The customer had licensed their existing PAM tool for a fraction of their actual user base. Against a technical user population that numbered in the hundreds, and thousands of total user objects in the directory, the tool had barely been rolled out. The architecture required to extend it wasn't worth the effort given what it couldn't do.
No path to agentic AI	The same architectural limitations blocking cloud coverage created a second, forward-looking problem. Agentic AI workloads require identities that can request access, act on resources, and complete tasks at machine speed, dynamically, and often across multiple systems in a single operation. A credential-centric PAM built for human administrators logging into static infrastructure has no model for that. There is no vault rotation schedule that matches millisecond-level agent actions. There is no session broker designed for a non-deterministic identity that may spawn sub-agents mid-task. For the customer, adopting agentic AI without solving the underlying identity and privilege architecture first would have meant building a new access model from scratch alongside the existing one, adding exactly the kind of fragmentation their security program was already working to address. The same tool that could not reach Snowflake and Databricks today would have had no answer for the AI workloads running on top of them tomorrow.

A renewal that changed the conversation

The catalyst was a renewal discussion with their existing PAM vendor. When the customer requested a modest number of additional licenses, the quoted per-user rate was significant enough to make a full renewal economically untenable. The projected cost for proper deployment was going to be multiples of what they were currently paying. This was a step-change increase, not an incremental one.

"PLAIN AND SIMPLE, IT'S RIDICULOUS. I HATE TO MISS AN OPPORTUNITY TO TAKE ADVANTAGE OF THAT STICKER SHOCK TO REINFORCE THE NEED TO CHANGE TOOLS."

The existing tool was ultimately renewed for just one year, with no new licenses purchased as the team began evaluating alternatives.

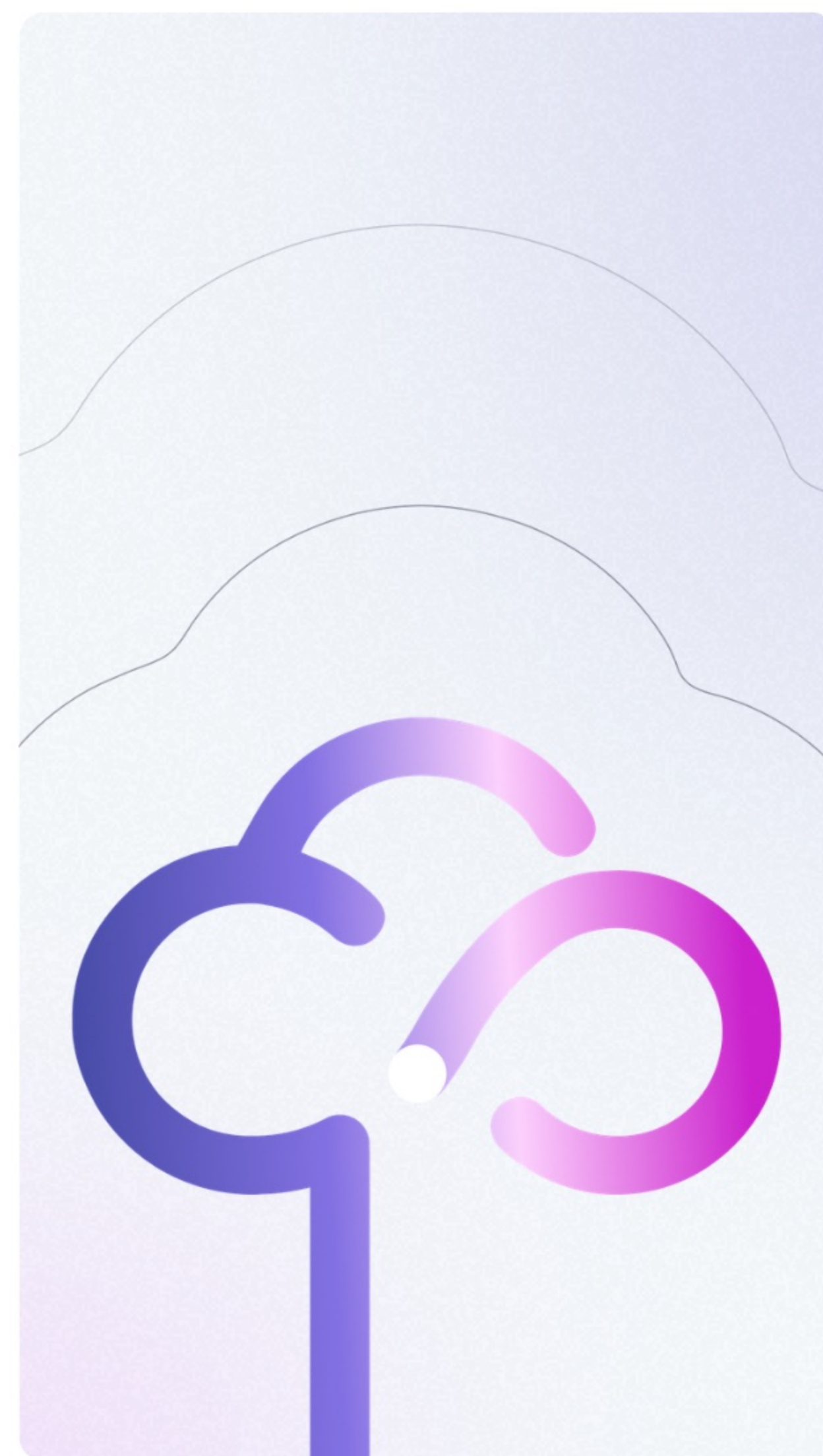
[02] WHY BRITIVE

The customer evaluated three vendors as required by internal policy. CyberArk was eliminated based on prior failed experience to meet the customer's requirements. The incumbent tool served as a baseline. Netwrix was considered as a third option. Britive was the second and quickly became the leading candidate.

The decision came down to architecture. Where connector, endpoint agent, and proxy-dependent PAM stores credentials and rotates them on a schedule, Britive enforces access at runtime: permissions are granted for the duration of a session and revoked automatically when the session ends. Nothing persists. There are no standing privileges to harvest.

For a team managing cloud platforms that their prior tool could not reach, a three-forest Active Directory environment, and an expanding set of non-human identities, this was the structural difference that mattered. The Global CISO, responded specifically to the just-in-time model and the concept of delegated responsibility: the ability to push privilege enforcement to the teams closest to the work, rather than concentrating it in a central vault.

The architecture's ability to extend to agentic AI was also a factor in the selection decision. The customer chose Britive in part because the same runtime enforcement model governing human users and non-human identities today applies to AI agents on the same architectural basis, with no separate platform, no separate policy engine, and no separate access model required as the environment evolves.



[03] DEPLOYMENT

From signed contract to live in just a few short weeks

Their existing PAM contract had a hard expiration. That created a forcing function: **the customer needed Britive deployed and functional before the existing tool went dark.**

The Britive implementation team ran near-daily working sessions from the start of the engagement. The migration was technically complex: the prior PAM tool had been configured over years in a tangled, non-standardized way across multiple AD forests, with service accounts, secrets, and access policies layered on top of each other. Untangling that and rebuilding it in Britive, while keeping the environment running, required close coordination between the Britive team and the customer's IAM engineers.

Britive went live in just a few weeks. For an environment of this complexity, that pace required deliberate planning and hands-on support from the implementation team.

PHASE 1 | Replicate and stabilize

The first phase focused on matching what the customer had in their prior tool, not improving it yet, but ensuring nothing broke during the transition. The team migrated:

 Domain admin accounts across their Active Directory environment, with password rotation and just-in-time access to servers	 Session recording, replacing the equivalent capability in the prior tool
 All secrets from the prior PAM vault, migrated to Britive Vault and organized with proper access controls, resolving the cross-team visibility problem where users could previously see each other's folders	 Automatic password rotation for target accounts, including a custom rotation capability built specifically for the customer that gives significantly more flexibility than vault-based PAM tools typically offer

On the password rotation capability specifically: vault-based PAM tools typically offer automatic rotation within fixed templates. Britive's implementation for the customer supports custom rotation scripts, configurable intervals, and dependency handling. When a password rotates, dependent services and connections are updated in the same operation. That flexibility was built for this customer and is now part of the platform.

PHASE 2 | Enforce just-in-time and eliminate standing access

Phase 2 is the current architectural shift, and the one that addresses the NHI security gap directly. Having stabilized usage on Britive, the team is now working through the environment systematically, replacing vaulted secrets and standing access with ephemeral, just-in-time access for both human users and non-human identities. This is where the migration from a static credential model to runtime privilege enforcement for NHIs becomes operational.

The targets include Active Directory, Oracle DB, Cisco network switches, and other infrastructure that currently runs on static non-human identity credentials. Each represents a machine identity that holds standing access today and will operate under runtime enforcement when Phase 2 is complete. In the target state:

 No standing access is granted to service accounts or their targets	 All access, human and non-human, is provisioned at runtime for the duration of the session
 When a session ends, permissions are revoked automatically	 If a credential is ever compromised, there are no persistent permissions attached to the account for an attacker to use

This is what true Zero Standing Privileges looks like in practice across a hybrid enterprise environment.

[04] RESULTS

~55% reduction in projected PAM spend	When the renewal quote came in from the incumbent vendor, the projected cost for a full deployment was enough to change the internal conversation entirely. The customer moved to Britive and covered twice the users across four cloud and on-premises environments, at a fraction of what staying would have cost.
2x more users covered	Britive doubled the number of users covered compared to what the prior tool had deployed, at a lower total cost and with active deployment underway rather than a tool sitting largely unused.
4x more environments covered	Where the prior PAM tool covered on-premises accounts only, Britive covers Azure, Snowflake, Databricks, and the on-premises infrastructure, with Salesforce and additional integrations in scope as the program matures. The cloud gap that had gone unaddressed for years is now being closed.
Platform enhancement delivered on an accelerated timeline	The flexible password rotation engine, supporting custom scripts, configurable intervals, and dependency handling, was built as a major platform enhancement on an accelerated timeline to meet the customer's go-live date. It is now available to all Britive customers as a standard platform capability. Enterprise deployments of this complexity tend to surface gaps in any platform. Britive's approach was to close them.
Deployment velocity that matched the business constraint	The existing contract expiration was a hard deadline with no flexibility. Britive went live in weeks across a three-forest AD environment with years of legacy configuration to migrate. The implementation pace was a function of close partnership and daily working sessions. This was not a simplified environment: three Active Directory forests, Azure, Snowflake, Databricks, and on-premises infrastructure managed through Britive's access broker, all migrated under a hard deadline with years of legacy configuration to untangle. This was not a simplified environment.

What comes next

Phase 2 is the long-term value of the engagement. As the customer moves from vault-based access to runtime privilege enforcement across the full environment, covering human users, service accounts, and eventually agentic workloads, the audit trail becomes automatic. Nothing persists past the session. Access is always current. Compliance reviews stop depending on manual reconciliation.

Agentic AI identity security was also a factor in the selection decision, not a future consideration. the customer evaluated Britive in part because the same runtime enforcement architecture that governs human users and non-human identities today applies to AI agents without requiring a separate platform or access model. As AI-driven workloads become part of their infrastructure, the ZSP framework already in place extends to cover them. This was a deliberate architectural choice: one runtime control point for human, agentic AI, and non-human identities, rather than adding a separate stack as the environment evolves.