>_ CUSTOMER PROOF

How Marqeta Traded JIT-on-Paper for Runtime Access Enforcement

Marqeta's prior tool checked the just-in-time box on paper while persistent accounts and week-long roles stayed behind. **Britive's runtime authorization and access enforcement now holds privileged accounts to Zero Standing Privileges** across AWS, Snowflake, and Salesforce, without slowing the engineers who keep its payment platform running.

MARQETA

100%

Of the cloud engineering workforce on one access control plane across Cloud & SaaS

Zero

Standing privileges held by human identities across critical infrastructure with privilege scoped to the duration of the task

Up to 40%

Estimated reduction in TCO by eliminating legacy vaulting infrastructure and dedicated platform staffing

> “Partnering with a mature solution like Britive helps us deliver true zero standing privileges at scale, with the speed our engineers expect and the security our customers deserve.”
>
> — CHETAN JHA, HEAD OF IDENTITY & VULNERABILITY SECURITY, MARQETA

ABOUT MARQETA

Marqeta is a global leader in modern card issuing, processing transactions for fintech companies and enterprises. It operates critical financial infrastructure, where access control is a core security posture decision rather than an operational footnote. Britive now secures privileged access for Marqeta's human cloud engineering workforce across AWS, Snowflake, and Salesforce under Zero Standing Privileges.

CONTENTS

[01] THE CHALLENGE

Just-in-time on paper, standing access in practice

On paper, Marqeta had just-in-time access. In practice, it had two pain points hiding under a checked box. The first: the JIT tool was entitlement-on-demand in disguise, with every engineer holding a persistent account and roles that lingered for up to a week, so the standing risk the tool was bought to remove was still there, masked rather than managed. The second: the brittle provisioning chain behind that tool was taxing engineering velocity every day, breaking under peak load and turning routine access into multi-system troubleshooting. Years of rapid growth had layered point solutions over Marqeta's most sensitive environments, and both pains traced back to that fragmentation.

To an outside observer, the box for just-in-time (JIT) access was technically checked. The engineering teams were using an access tool designed to limit standing risk. But a closer look at the mechanics showed the reality did not match the promise of true just-in-time access.

PAIN POINT ONE | Just-in-time in name only

Entitlement-on-demand, not JIT	Every developer and engineer still held a persistent, standing account inside AWS. When they authenticated, they simply arrived without a role attached.
Roles that lingered	When a user requested access, the tool attached the required role, and then that role stayed attached, often for up to seven days. The underlying accounts never left the environment.
Risk masked, not removed	Because access was deemed temporary on paper, the tool was used as justification to bypass thorough access reviews. For critical financial infrastructure, that model was mismatched for the long game.

The friction was not confined to lingering access. It bled into daily engineering velocity. The prior tool relied on a complex, multi-hop provisioning chain, and every step added a way for access to break.

PAIN POINT ONE | The compounding operational cost

Brittle multi-hop provisioning	A checkout triggered an API call to the identity provider, which pushed the user ID into a push group, which then synced into AWS. Two hops, multiple points of failure.
Rate-limit bottlenecks	During peak deployment hours, simultaneous checkouts routinely hit identity provider rate limits. If the directory service had even a minor hiccup, the entire access pipeline collapsed, locking engineers out of production.
Troubleshooting overhead	A single access ticket required engineers to audit across three systems instead of two, adding more than 30% to day-to-day troubleshooting complexity, by the team's estimate.

> We were paying for just-in-time access but getting multi-system bottlenecks. If our access model was breaking under the weight of our daily engineering deployments, there was zero chance it could deliver the speed and scale AI adoption demands securely or otherwise.
>
> — CHETAN JHA, HEAD OF IDENTITY & VULNERABILITY SECURITY, MARQETA

The before state carried a cost across the three categories that matter most: software, infrastructure, and people. At that cost, the control it was all buying did not exist as advertised: Marqeta was paying for just-in-time and receiving entitlement-on-demand. By replacing its brittle multi-hop provisioning chain with Britive's SaaS-delivered native enforcement, Marqeta successfully collapsed the traditional Privileged Access Management (PAM) TCO model.

Software Consolidation

Legacy access tools typically require heavy recurring fees, often $70 to $200+ per privileged user annually, layered with expensive module add-ons. By moving to a unified access surface, Marqeta shed the licenses for the JIT point tool and the niche tools layered around it.

Infrastructure Elimination

Complicated design that includes multiple hops across multiple systems results in unnecessary break points impacting engineering response time in case of incidents. Britive's architecture removed the active intermediary from the live path. This eliminated the directory push-group plumbing the whole provisioning chain depended on.

People & Operational Overhead

In legacy deployments, staffing frequently constitutes 30% to 40% of the five-year TCO, demanding dedicated engineers just to manage platform integrations and troubleshoot connectivity failures.
By natively enforcing access, Marqeta eliminated the more than 30% added troubleshooting complexity by the team's estimate. Every access ticket is now deterministic, rather than spanning three systems, reclaiming engineering hours lost to peak-hour lockouts.

Estimated TCO Impact: Legacy PAM vs. True ZSP

COST CATEGORY	LEGACY PAM / ENTITLEMENT-ON-DEMAND MODEL	THE BRITIVE NATIVE ZSP MODEL
Software Licensing	High baseline costs with forced modular add-ons	Consolidated coverage across AWS, Snowflake, and Salesforce
Infrastructure	Heavy (dedicated proxies, SQL/OS licenses, session storage)	Zero footprint (native cloud enforcement)
Dedicated Staffing	2 to 3 specialized IAM/PAM engineers required	Reallocated to core security engineering; no dedicated platform babysitters
Troubleshooting	High (multi-system audit trails and rate-limit bottlenecks)	Deterministic troubleshooting confined to two systems

Marqeta's leadership recognized that this trajectory was unsustainable. The organization did not need another niche tool layered on a fragile pipeline. It needed a single, unified runtime control plane that could enforce native, zero-standing access at scale without slowing down development teams.

[02] THE SOLUTION

Runtime privilege enforcement

Marqeta deployed Britive as the unified runtime privilege access control plane across its most critical infrastructure: AWS, Snowflake, and Salesforce. The core shift was architectural. Britive removed the active intermediary from the live path. Instead of a fragile chain of directory groups and proxied API calls, it authorized and enforced policies natively, directly on the target systems. Authorization decides, enforcement acts.

From entitlement-on-demand to true ZSP	Persistent developer accounts were removed from AWS. Access policy now exists independently of identity presence. An approved request grants a window of time, not active access. The role is provisioned natively at the moment work begins, and stripped away the moment the session closes. Nothing lingers.
A unified access surface	Marqeta replaced AWS Identity Center with the Britive dashboard. The full human cloud engineering workforce moved to this single access surface, so engineers no longer navigate multiple consoles just to find the access they need.
Security written as code	To match modern cloud-native development practice, the entire deployment was anchored in Terraform. Access policies live in the codebase, version-controlled and subjected to the same peer-review standards as any production configuration change.
Built mid-deployment: PagerDuty-aware access	Mid-deployment, Marqeta surfaced a non-negotiable requirement: engineers on call in PagerDuty needed immediate elevated access for incident response without waiting on a manual approval workflow. That capability did not exist in Britive at the time. Rather than queue it for a multi-quarter roadmap, Britive's product and engineering teams built and delivered a native, PagerDuty-aware capability ahead of go-live, in a matter of weeks. It is now a standard part of the platform. When an engineer is on call, Britive verifies that status at runtime and grants access immediately, while maintaining a strict zero-standing posture for everyone else.

[03] THE RESULTS

Eliminate standing privileges at scale

The systemic friction that used to define the access lifecycle has been replaced by a quiet, predictable rhythm. Each result answers a pain point that drove the project. The masked risk is gone for real: no persistent accounts, no lingering roles, true Zero Standing Privileges. And the velocity tax is gone with it: the brittle chain is out of the live path, rate limits no longer gate deployment hours, and troubleshooting is deterministic. Marqeta closed its standing-access exposure, removed the brittle provisioning chain, and gave engineers a faster path to the access they need.

Attack Surface Reduction

Across AWS, Snowflake, and Salesforce, the engineering team operates under Zero Standing Privileges. The multi-day standing roles that once left a continuous footprint are gone, replaced by short-lived privilege scoped to active work.

Zero

RATE-LIMIT BOTTLENECKS

By bypassing directory infrastructure for live provisioning, Marqeta eliminated API rate-limiting bottlenecks. Troubleshooting is deterministic, confined to two systems instead of a web of intermediaries.

1 Common Access & Policy Model

The human cloud engineering workforce operates from a single dashboard across AWS, Snowflake, and Salesforce, instead of navigating multiple tool-specific consoles.

BUILT IN WEEKS, BEFORE GO-LIVE

PagerDuty-aware access did not exist in the platform when Marqeta named it a non-negotiable. Britive built and delivered it ahead of go-live: on-call status verified at runtime, immediate elevated access for incident response, zero standing posture for everyone else. New capability for this customer, now a standard part of the platform.

Evidence by architecture

Because access is created at runtime and removed when the session closes, the audit trail stays current by design. Every session is built on dynamic checkouts, so granular audit records are generated automatically at runtime, giving compliance teams clean verification data directly alongside native cloud infrastructure logs.

THE MATH EVERYONE IS DOING

When stolen credentials are the way in, the average breach runs 246 days from intrusion to containment (IBM Cost of a Data Breach Report 2025). At Marqeta, the role is stripped the moment the session closes. There is no persistent account to compromise, and no eight-month window for one to be used.

[04] BEFORE / AFTER

BEFORE BRITIVE	AFTER BRITIVE
Entitlement-on-demand: persistent AWS accounts with roles attached for up to seven days	True Zero Standing Privileges: no persistent accounts; the role is provisioned at the moment work begins and stripped at session close
Multi-hop provisioning routed through an identity provider's push groups into AWS	Native enforcement directly on the target system, with the intermediary removed from the live path
Peak-hour checkouts hitting identity provider rate limits; any hiccup collapsed the pipeline	Rate-limit bottlenecks eliminated; provisioning no longer depends on directory infrastructure
One access ticket spanning three systems to troubleshoot	Deterministic troubleshooting confined to two systems
Multiple tool-specific consoles to find access	One unified access surface for the human cloud engineering workforce
On-call access through standing permissions or manual approval queues	PagerDuty-aware checkout: on-call status verified at runtime, immediate access, zero standing for everyone else
Standing privilege deemed temporary on paper, masking risk	Short-lived privilege scoped to active work, with audit records generated automatically at runtime

THE TAKEAWAY

For Marqeta, the journey was not about enforcing restrictive security barriers. It was about building an architectural foundation clean enough to support rapid enterprise velocity.