

LIVE AZURE VALIDATION

When an agent exceeds its authority.

APEX enforced the boundary.

The test

One approved customer lookup. Attempts to change its target, reuse authorization, and exceed granted access.

The evidence

Five SQL checks passed against a real Azure database using synthetic customer records.

THE ACCESS BOUNDARY

One permitted customer. Two database records.

The caller has narrower authority.

Gateway identity

Read access to both synthetic records. No INSERT, UPDATE or DELETE permission on the Customers table.

Caller policy

Read access to customer 910001 only. Customer 910002 remains outside the caller's grant.

SQL RESULTS / SEPTEMBER 24, 2026

Approved access succeeds.

Restricted access is denied.

200 / PASS

Customer 910001 returned the exact expected synthetic record.

403 / PASS

Customer 910002 was denied by the resource policy, despite the gateway identity being able to read it.

SIGNED EXECUTION

The authorization binds the request.

Changes and replays are rejected.

403 / PASS

Changing the customer ID invalidated the signed authorization. The original request still succeeded: 200 / PASS.

409 / PASS

Reusing a completed execution was rejected. A valid identity token alone does not authorize an execution.

SEPARATE RESTART AND CONCURRENCY TESTS

A restart does not reset authority.

Persistent state preserves the limits.

After container replacement

Used execution: 409. Exhausted budget: 403. Fresh authorized execution: 200.

Concurrent attempts

For duplicate execution and a one-action budget, each six-request test allowed one and rejected five.

SCOPE AND NEXT STEPS

Evidence for specific controls.

A clear boundary for the claim.

Demonstrated

Governed SQL access, signed argument binding, replay rejection, and persistent task budgets in the isolated Azure test app.

Next containment milestone

Test direct paths around the gateway and isolation of credentials and signing material. Artifactory was not tested.