

CHG0030005 — [TITAN] High — security on dbw-titan-analytics

Severity	High	Priority	2 - High
Cloud	Azure	State	New
Resource	dbw-titan-analytics	Group	data_platform
Resource type	Microsoft.Databricks/workspaces	Change type	Normal
Opened	2026-04-21 14:36:43	Closed	2026-04-21 14:36:43
CAB required	Yes	Close code	—

Security Finding

Databricks workspace 'dbw-titan-analytics' has public network access enabled and no VNet injection – cluster traffic leaves the Azure backbone.

Justification

Databricks workspace 'dbw-titan-analytics' has public network access enabled and no VNet injection – cluster traffic leaves the Azure backbone.

Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
Re-deploy workspace with enableNoPublicIp=true + customVirtualNetworkId set to rg-titan-demo/vnet-titan-data/snet-databricks-private
3. TITAN FORGE verifies the fix was applied.
4. Post-change rescan by TITAN SCOUT – finding must no longer appear.
5. Close ticket with Successful close_code.

Risk & Impact Analysis

Risk level: MEDIUM-HIGH risk – misconfiguration with realistic exploit path.
Business impact if unremediated: Increases attack surface; auditor finding likely.
Scope: single resource (dbw-titan-analytics).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Databricks workspace 'dbw-titan-analytics' has public network access enabled and no VNet injection – cluster traffic leaves the Azure backbone.

Backout / Rollback Plan

1. TITAN auto-captured snapshot of dbw-titan-analytics before change (baseline: titan-live-demo-20260421T213642Z).
2. If post-change rescan still shows the finding OR a new issue appears within 15 min:
 - a. TITAN FORGE fires rollback automatically using stored snapshot.
 - b. Incident reopens and escalates to on-call.
3. Manual rollback command path (human override) is documented in close notes.

Test Plan

1. TITAN SCOUT rescans dbw-titan-analytics immediately after FORGE applies the change.
2. PASS criteria: the specific finding no longer appears in SCOUT results.
3. PASS criteria: no new CRITICAL or HIGH findings introduced by the change.

4. Automated compliance check: HIPAA/PCI/SOC2 controls re-evaluated.
5. If any check fails, backout plan fires automatically.

Recommended Fix Command

Re-deploy workspace with enableNoPublicIp=true + customVirtualNetworkId set to rg-titan-demo/vnet-titan-data/snet-databricks-private

Compliance Mapping

CIS 1.x IAM, NIST AC-2, SOC 2 CC6.1

AI Close Notes

(empty)