SecureOps RiskScore 360

Security Assessment Report

Generated: 2026-01-04 10:18:05 UTC
Subscription: b6df8227-8888-4209-a122-e75503b5516e
Resource Group: repport3

1. Executive Summary

25
Risk Level: Medium

This report consolidates governance compliance (Azure Policy), identity governance (RBAC/IAM), Defender for Cloud posture, and selected exposure controls (network & encryption) into a normalized risk score to support remediation prioritization.

Top Risk Drivers:

- IAM: 35 points (critical)

2. Score Breakdown

Component	Value	Evidence (Real Inputs)
Policy	0	0 unique non-compliant policies
IAM	35	Drift: owner | Owners: 10 | Contributors: 9 | Readers: 2
Defender	0	Unhealthy: High=0, Medium=0, Low=0
Network	0	Open risky ports: 0 | Public IPs: 0 | Missing NSG: 0
Encryption	0	Unencrypted storage: 0 | Weak TLS: 0
Total (Normalized)	25	Raw: 35 / 135 | Level: Medium

3. Recommended Actions (Prioritized)

1. Reduce privileged sprawl: review RBAC assignments. Current counts -> Owners=10, Contributors=9. Keep Owner role for break-glass/admin accounts only.

Technical Appendix - Evidence & Methodology

A. Data Sources & Scope

Azure Policy: Microsoft.PolicyInsights policyStates (NonCompliant) at resource-group scope. IAM/RBAC: Microsoft.Authorization roleAssignments at subscription scope. Defender for Cloud: Microsoft.Security assessments (Unhealthy only) at RG scope. Network: NSG rules, NIC protection, public IP exposure. Encryption: storage account encryption, TLS, and HTTPS enforcement.

B. Top Non-Compliant Policies (by records)

No policy data available.

C. IAM Evidence (samples)

Drift: owner. Owners=10, Contributors=9, Readers=2. Samples below.

Owner principals (sample)

Principal ID	Type
246d6963-1c7a-4d45-860f-0fa9e9e4913d	User
ce2a45e3-6cec-4d92-9ebb-b52fec12c3b0	ServicePrincipal
5e7d13ff-89ce-484f-a9a9-b5281648ff49	ServicePrincipal
a4b09772-201e-417f-8221-aa80f77035f9	User
83c3b00a-7d0b-4d59-a5dc-8d09242f5bd7	User
966dc3e7-210a-4117-a638-75f2c27ddf53	User
ce6795c4-0294-4088-8fe2-2538ea58beb2	User
f27c8a13-a0b7-4414-a8cb-1f2966bfd42b	User

Contributor principals (sample)

Principal ID	Type
ce2a45e3-6cec-4d92-9ebb-b52fec12c3b0	ServicePrincipal
63121f61-e2be-4393-9a29-2b019c6dfe2e	ServicePrincipal
a5748043-2b88-4637-bb60-51c95be66b0e	ServicePrincipal
cc8e4cbe-1e4b-4ee4-934c-441c6df44d5f	ServicePrincipal
246d6963-1c7a-4d45-860f-0fa9e9e4913d	User
25f17dd1-197e-48ee-8a20-b3f5fedf8f17	User
83c3b00a-7d0b-4d59-a5dc-8d09242f5bd7	User

D. Scoring Methodology (Normalized)

- Each component produces a bounded sub-score: Policy(0-40), IAM(0-35), Defender(0-35), Network(0-15), Encryption(0-10).
- Raw total = sum(component scores). Max possible = 135.
- Final RiskScore = min(100, round((RawTotal / 135) × 100)).
- Risk Level thresholds: Low<10, Low-Medium<25, Medium<40, Medium-High<60, High<75, Critical≥75 (or critical component + score≥50).

E. Notes & Limitations

Defender counts may be 0 if Defender for Cloud is not enabled or not fully initialized. IAM drift is computed using threshold-based heuristics and should be tuned to organizational baselines. Network/encryption checks depend on RBAC permissions and available resources in the RG.