StageAuto Report

Infrastructure Risk Analysis for Terraform Environments

Generated at: 2026-04-08 04:04:03 UTC

Executive Summary

This report identifies critical security, compliance, and cost risks in your cloud infrastructure. Unresolved issues may lead to data breaches, financial loss, or regulatory violations.

Overall Risk Score: 18/100 (CRITICAL)

Top Priorities

1. **CRITICAL** — Public Access to Sensitive Port (22) (aws_security_group.app)
2. **CRITICAL** — Public S3 Bucket (aws_s3_bucket.uploads)
3. **CRITICAL** — Compliance Risk: Public Storage (aws_s3_bucket.uploads)
4. **HIGH** — Public Subnet (Auto Public IP) (aws_subnet.public)
5. **HIGH** — Database Not Encrypted (aws_db_instance.db)

■ SECURITY

[HIGH] Public Subnet (Auto Public IP)

Resource: aws_subnet.public
Why this matters: Resources launched here may be exposed to the internet.
What's wrong: Subnet automatically assigns public IPs.
How to fix: Disable map_public_ip_on_launch or use private subnets.

[CRITICAL] Public Access to Sensitive Port (22)

Resource: aws_security_group.app
Why this matters: Attackers can attempt brute-force or direct access to your infrastructure.
What's wrong: Port 22 is exposed to the public internet.
How to fix: Restrict access to specific IP ranges or use a bastion host.

[CRITICAL] Public S3 Bucket

Resource: aws_s3_bucket.uploads
Why this matters: Sensitive data may be exposed to the internet.
What's wrong: Bucket is publicly accessible.
How to fix: Set ACL to private and restrict access using IAM policies.

[HIGH] Database Not Encrypted

Resource: aws_db_instance.db
Why this matters: Sensitive data may be exposed if storage is compromised.
What's wrong: Database storage is not encrypted.
How to fix: Enable storage_encrypted = true.

[HIGH] HTTP Without HTTPS

Resource: aws_lb_listener.http_listener
Why this matters: Traffic is not encrypted in transit.
What's wrong: Load balancer is using HTTP instead of HTTPS.
How to fix: Use HTTPS with SSL/TLS certificates.

[MEDIUM] HTTPS Not Enforced

Resource: global
Why this matters: Traffic may be transmitted without encryption.
What's wrong: No HTTPS listener detected in infrastructure.
How to fix: Configure HTTPS listeners (SSL/TLS) for secure communication.

■ ARCHITECTURE

[HIGH] S3 Bucket Versioning Not Enabled

Resource: aws_s3_bucket
Why this matters: Risk of permanent data loss due to accidental deletion, overwrite, or ransomware events.
What's wrong: One or more S3 buckets were detected without versioning enabled.
How to fix: Enable S3 bucket versioning to protect against accidental or malicious object deletion.

[MEDIUM] S3 Bucket Encryption Not Explicitly Configured

Resource: aws_s3_bucket
Why this matters: Data stored at rest may not meet security or compliance requirements.
What's wrong: S3 buckets were detected without explicit server-side encryption configuration.
How to fix: Enable server-side encryption using AWS-managed or customer-managed KMS keys.

[MEDIUM] Database Not Using Multi-AZ

Resource: aws_db_instance.db
Why this matters: Reduced availability and resilience in case of failure.
What's wrong: Database is not configured for Multi-AZ deployment.
How to fix: Enable multi_az = true for production workloads.

■ COMPLIANCE

[CRITICAL] Compliance Risk: Public Storage

Resource: aws_s3_bucket.uploads

Why this matters: Higher probability of audit findings, policy non-compliance, data exposure incidents, and regulatory consequences.

What's wrong: A storage resource was detected as public. This commonly violates security baselines (e.g., CIS) and audit controls (e.g., SOC 2 / ISO 27001). Depending on data type, it may also introduce privacy and regulatory risk.

How to fix: Make the resource private, enforce IAM access controls, review data classification, and apply policies that prevent public access by default.

■ COST OPTIMIZATION

[MEDIUM] Cost Risk: Public Bucket Can Increase Traffic

Resource: aws_s3_bucket.uploads

Why this matters: Higher chance of billing surprises and unnecessary spend.

What's wrong: Public buckets may generate unexpected downloads and requests, which can increase variable costs (data transfer/egress and request fees).

How to fix: Make the bucket private, enable logging/monitoring, review access patterns, and apply budget alerts to catch unexpected usage early.