STRONDEX

AWS Security Hardening — Top 10 Controls

The highest-impact controls, pulled from our 95-point AWS Security Hardening checklist.

Start here. These are the controls that block the most risk (and the ones auditors and cyber-insurance carriers ask about first). Work top-down — severity is highest at the top.

1	CRITICAL	**Enable MFA on the root account.** **Verify:** In IAM → Security recommendations (or sign in as root → My Security Credentials), confirm MFA is registered.
2	CRITICAL	**Ensure no access keys exist on the root account.** **Verify:** Sign in as root → My Security Credentials → Access keys, or run aws iam get-account-summary and check AccountAccessKeysPresent = 0.
3	CRITICAL	**Do not use the root account for day-to-day work.** **Verify:** Review the IAM credential report (aws iam generate-credential-report) for recent root password_last_used.
4	CRITICAL	**Attach no IAM policies directly to users — use groups or roles.** **Verify:** Run aws iam list-attached-user-policies per user (and check inline policies).
5	CRITICAL	**Enable CloudTrail in all regions.** **Verify:** CloudTrail → Trails → Create trail with Apply to all regions enabled (a multi-region trail).
6	CRITICAL	**Enable CloudTrail log file integrity validation.** **Verify:** On the trail, turn on Log file validation (--enable-log-file-validation).
7	CRITICAL	**No Security Group allows SSH (port 22) from 0.0.0.0/0.** **Verify:** EC2 → Security Groups: find inbound rules for port 22 with source 0.0.0.0/0 or ::/0.
8	CRITICAL	**No Security Group allows RDP (port 3389) from 0.0.0.0/0.** **Verify:** Same review for port 3389.
9	CRITICAL	**Enable account-level S3 Block Public Access (all four settings).** **Verify:** S3 → Block Public Access settings for this account: turn on all four toggles.
10	CRITICAL	**No S3 bucket is publicly readable (no s3:GetObject for principal *).** **Verify:** Use IAM Access Analyzer for S3 or the bucket list's Access column to find public-read buckets.