STRONDEX

Azure Security Hardening — Top 10 Controls

The highest-impact controls, pulled from our 88-point Azure 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	**Require multi-factor authentication for every user.** **Verify:** In the Microsoft Entra admin center → Protection → Conditional Access, confirm a policy requires MFA for all users (or enable Security Defaults under…
2	CRITICAL	**Enforce MFA on every Global Administrator account.** **Verify:** Under Entra → Roles and administrators → Global Administrator, list members, then confirm a Conditional Access policy targeting admin roles requires M…
3	CRITICAL	**Block legacy authentication protocols.** **Verify:** Create a Conditional Access policy under Protection → Conditional Access with Client apps = Exchange ActiveSync clients + Other clients and grant Bloc…
4	CRITICAL	**Require MFA for all users via Conditional Access.** **Verify:** In Protection → Conditional Access → Policies, confirm an enabled policy with Users = All users (break-glass excluded), Cloud apps = All, and grant Re…
5	CRITICAL	**Block legacy authentication via Conditional Access.** **Verify:** Confirm an enabled CA policy targeting Other clients / Exchange ActiveSync with grant Block (the enforcement complement to AZ-ID-03).
6	CRITICAL	**Don't grant subscription Owner to users who don't need it.** **Verify:** In Subscription → Access control (IAM) → Role assignments, filter to the Owner role, or run az role assignment list --role Owner --scope /subscription…
7	CRITICAL	**Retain the Azure Activity Log for at least one year.** **Verify:** The Activity Log keeps 90 days by default.
8	CRITICAL	**No NSG allows unrestricted inbound SSH (port 22) from the internet.** **Verify:** Review Network security groups → Inbound security rules for any rule allowing TCP 22 from source Any / 0.0.0.0/0 / Internet.
9	CRITICAL	**No NSG allows unrestricted inbound RDP (port 3389) from the internet.** **Verify:** Same review as above for TCP 3389.
10	CRITICAL	**Disable public blob access on storage accounts.** **Verify:** In Storage account → Settings → Configuration, set Allow Blob public access = Disabled, or run az storage account update --allow-blob-public-access fa…