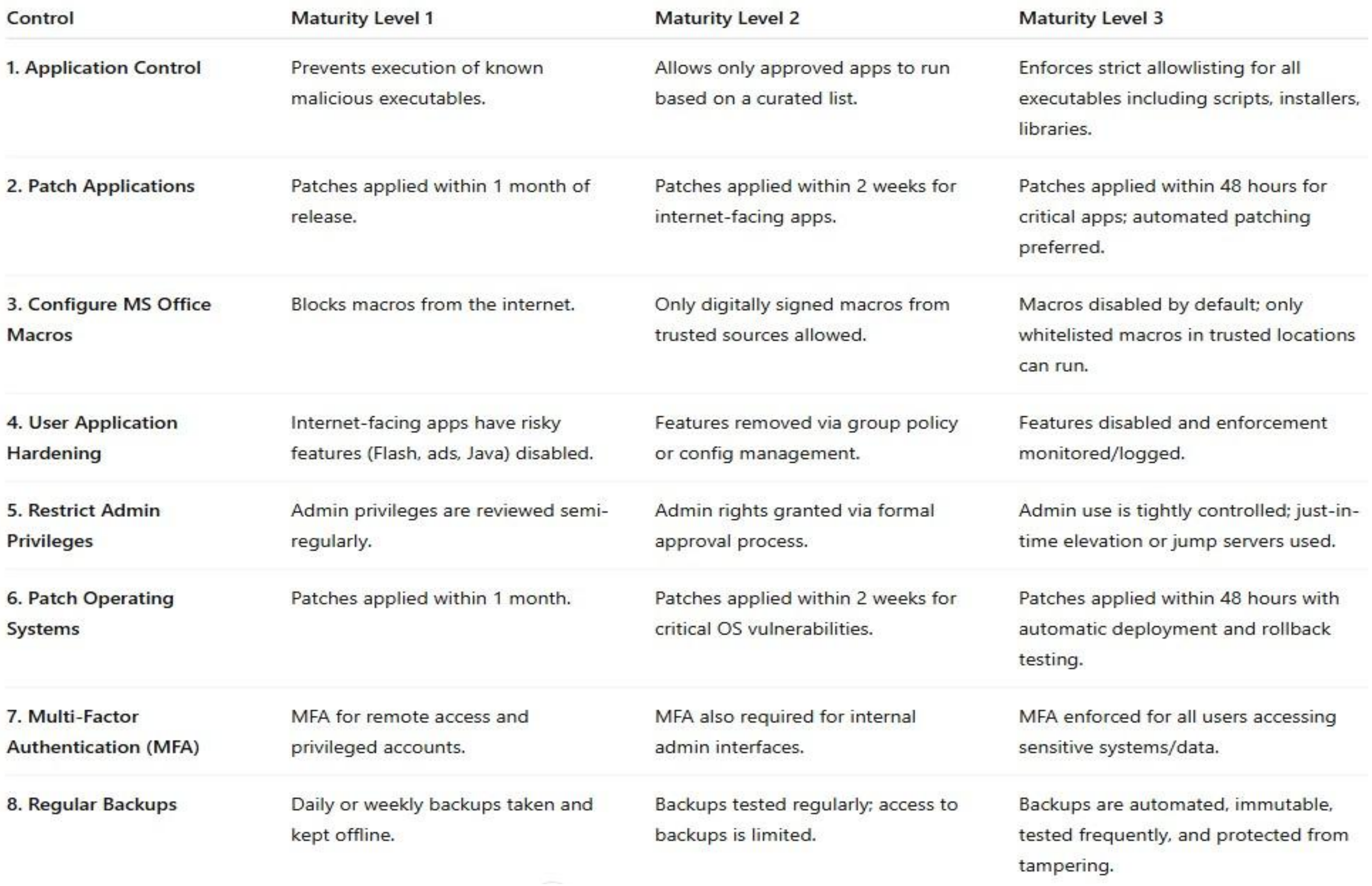

Control	Maturity Level 1	Maturity Level 2	Maturity Level 3
1. Application Control	Prevents execution of known malicious executables.	Allows only approved apps to run based on a curated list.	Enforces strict allowlisting for all executables including scripts, installers, libraries.
2. Patch Applications	Patches applied within 1 month of release.	Patches applied within 2 weeks for internet-facing apps.	Patches applied within 48 hours for critical apps; automated patching preferred.
3. Configure MS Office Macros	Blocks macros from the internet.	Only digitally signed macros from trusted sources allowed.	Macros disabled by default; only whitelisted macros in trusted locations can run.
4. User Application Hardening	Internet-facing apps have risky features (Flash, ads, Java) disabled.	Features removed via group policy or config management.	Features disabled and enforcement monitored/logged.
5. Restrict Admin Privileges	Admin privileges are reviewed semi-regularly.	Admin rights granted via formal approval process.	Admin use is tightly controlled; just-in-time elevation or jump servers used.
6. Patch Operating Systems	Patches applied within 1 month.	Patches applied within 2 weeks for critical OS vulnerabilities.	Patches applied within 48 hours with automatic deployment and rollback testing.
7. Multi-Factor Authentication (MFA)	MFA for remote access and privileged accounts.	MFA also required for internal admin interfaces.	MFA enforced for all users accessing sensitive systems/data.
8. Regular Backups	Daily or weekly backups taken and kept offline.	Backups tested regularly; access to backups is limited.	Backups are automated, immutable, tested frequently, and protected from tampering.