Software Security	Authenticated user	Encrypted data streams	Storage encryption	Verified firmware
Hardware Security	ARM TrustZone CPU	TPM	Unique ID	