Highly Secure Access Ensuring Only True Identity Logs In
Enforce SSO (Single Sign-On) for all apps
Require MFA (Multi-Factor Authentication) / passkeys for staff/admins; phase to field
Role/Attribute-Based Access Control
JIT (Just-In-Time) elevation & PAM (Privileged Access Management) for consoles/DBs
Break-glass accounts with monitoring
Integration Security
All APIs terminate at an API gateway (auth, schema, rate limit, logging)
OAuth 2.0 + JWT (JSON Web Token) with narrow scopes & tenant claims
mTLS (mutual TLS) with critical partners (wallet/KYC)
Webhooks: HMAC-signed over raw body + timestamp/nonce + replay window
Idempotency keys on mutating endpoints
Authorization tests for BOLA/BFLA (Broken Object/Function-Level Authorization)
Ship Clean Code (Secure Delivery)
SAST/DAST/SCA (Static/Dynamic/App-deps) in Continuous Delivery
Secrets scanning & prevention
SBOM (Software Bill of Materials) + signed artifacts
IaC (Infrastructure as Code) policy gates (OPA/Checkov) for Terraform/CloudFormation
Know Your Data (Discovery & Protection)
DSPM discovery & classification of PII/KYC/payout/genealogy
Encrypt in transit & at rest; keys in KMS (Key Management Service)
Tokenize sensitive fields; store only tokens & last-4 where needed
Log redaction (no PAN/IDs in logs/traces/tickets)
Automated retention & deletion (KYC images, exports)
Cloud Protection
CSPM (Cloud Security Posture Management): deny public buckets, require encryption
Private endpoints (e.g., AWS PrivateLink/Azure Private Link)
Alert on sensitive data in wrong buckets
Fortify Storefronts (Web Front-End)
Content Security Policy
HSTS (HTTP Strict Transport Security)
Hosted payment fields/iFrames
Pass PCI with Less Pain (Cardholder Data)
Stop the Leaks (Sharing Controls)
Export linked to the requester's identity
Watermark & time-limit exports; minimize CSV columns
Alert on mass exports & unusual download patterns
Protect the Money (Fraud & Payouts)
Aligning payouts with KYC information
flagging suspicious patterns
Step-up MFA for sensitive actions (payout edits, large runs)
Daily reconciliation across wallet, bank, internal ledger
Velocity/device anomaly detection on orders & payouts
Quick Detection and Right Response

Security Information and Event Management with high-signal rules
Endpoint Detection & Response on servers/endpoints
User & Entity Behavior Analytics
Run on Governance (Program & Evidence)
Written Information Security Program
Control→evidence mapping & quarterly leadership reports
Automate evidence collection