**Security Features Implementation**

**Key Security Features Implemented in Code:**

* **Authentication:**
  + OAuth2.0 via Keycloak/Auth0 integration
  + Refresh token mechanism for session continuation
  + MFA optional layer with TOTP/Email OTP
* **Authorization:**
  + Role-Based Access Control (RBAC)
  + Scoped permissions (e.g., CAN\_CREATE\_CASE, CAN\_VIEW\_REPORTS)
  + Middleware interceptors for endpoint access filtering
* **Data Protection:**
  + AES-256 encryption for PII and sensitive notes
  + Passwords hashed using bcrypt
  + SSL certificates (Let's Encrypt in dev, custom CA in prod)
* **Security Testing:**
  + Static Code Analysis (e.g., SonarQube)
  + Penetration test script coverage for endpoints (via OWASP ZAP)
  + Security headers set via middleware: X-Frame-Options, Strict-Transport-Security, Content-Security-Policy