ONYX Platform  
Security Architecture Document

Comprehensive Security Framework  
for Building Assessment Platform

**Platform: onyxreport.com  
Security Level: Enterprise Grade**

Document Version: 1.0  
Last Updated: August 2025  
Classification: Confidential  
Prepared by: ONYX Security Team

ONYX Platform Security Architecture Document

**Document Version:** 1.0

**Last Updated:** August 2025

**Classification:** Confidential

**Platform:** onyxreport.com

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Executive Summary

The ONYX Platform has implemented a comprehensive, enterprise-grade security architecture that addresses modern cybersecurity threats and compliance requirements. This document outlines the multi-layered security framework protecting the building assessment and lifecycle reporting platform.

Security Objectives

- **Confidentiality**: Protect sensitive building and assessment data

- **Integrity**: Ensure data accuracy and prevent unauthorized modifications

- **Availability**: Maintain 99.9% uptime with resilient infrastructure

- **Compliance**: Meet SOC 2, GDPR, and industry standards

- **Auditability**: Comprehensive logging and monitoring

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Security Architecture Overview

1.1 Defense-in-Depth Strategy

The ONYX platform employs a layered security approach with multiple defensive barriers:

┌─────────────────────────────────────────────────────────────────┐

│ Internet/External Users │

├─────────────────────────────────────────────────────────────────┤

│ Layer 1: Cloudflare WAF & DDoS Protection │

│ - Bot mitigation, rate limiting, geo-blocking │

├─────────────────────────────────────────────────────────────────┤

│ Layer 2: SSL/TLS Encryption (HTTPS) │

│ - TLS 1.3, HSTS, Certificate pinning │

├─────────────────────────────────────────────────────────────────┤

│ Layer 3: Application Security Headers │

│ - CSP, X-Frame-Options, XSS Protection │

├─────────────────────────────────────────────────────────────────┤

│ Layer 4: API Gateway & Authentication │

│ - JWT tokens, 2FA, session management │

├─────────────────────────────────────────────────────────────────┤

│ Layer 5: Application Security Controls │

│ - Input validation, SQL injection prevention, XSS protection │

├─────────────────────────────────────────────────────────────────┤

│ Layer 6: Database Security │

│ - Encrypted connections, access controls, audit logging │

└─────────────────────────────────────────────────────────────────┘

1.2 Technology Stack Security

**Frontend Security (React/TypeScript)**

* Content Security Policy (CSP)
* Subresource Integrity (SRI)
* XSS protection mechanisms
* Secure cookie handling

**Backend Security (Node.js/Express)**

* Helmet.js security headers
* Rate limiting and throttling
* Input validation and sanitization
* SQL injection prevention

**Database Security (PostgreSQL)**

* Encrypted connections (SSL/TLS)
* Row-level security policies
* Audit logging
* Backup encryption

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. Authentication & Authorization Framework

2.1 Multi-Factor Authentication (MFA)

**Primary Authentication**

* Secure password policies (8+ characters, complexity requirements)
* Bcrypt hashing with salt (rounds: 10)
* Account lockout after 5 failed attempts

**Two-Factor Authentication (2FA)**

* Time-based One-Time Passwords (TOTP)
* Support for Google Authenticator, Authy, Microsoft Authenticator
* Backup recovery codes (10 single-use codes)
* QR code generation for easy setup

**Implementation Details:**

// 2FA Token Generation

const secret = speakeasy.generateSecret({

name: `ONYX Platform (${userEmail})`,

issuer: 'ONYX Platform',

length: 32

});

// Token Verification

const verified = speakeasy.totp.verify({

secret: userSecret,

encoding: 'base32',

token: userToken,

window: 2 // ±60 seconds tolerance

});

2.2 Role-Based Access Control (RBAC)

**User Roles:**

- **Admin**: Full system access, user management, security configuration

- **Manager**: Organization management, team oversight, assessment review

- **Assessor**: Assessment creation, building data entry, report generation

**Permission Matrix:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Resource** | **Admin** | **Manager** | **Assessor** |
| User Management | ✓ | ✓ (org only) | ✗ |
| Security Config | ✓ | ✗ | ✗ |
| All Organizations | ✓ | ✗ | ✗ |
| Own Organization | ✓ | ✓ | ✓ |
| Assessments | ✓ | ✓ (read/review) | ✓ (create/edit) |
| Buildings | ✓ | ✓ | ✓ (limited) |
| Reports | ✓ | ✓ | ✓ (own only) |

2.3 Session Management

**Session Security Features:**

* JWT tokens with 7-day expiration
* Refresh tokens with 30-day expiration
* Automatic token rotation
* Session tracking and concurrent session limits
* Secure cookie attributes (HttpOnly, Secure, SameSite)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Data Protection & Encryption

3.1 Encryption in Transit

**TLS/SSL Implementation:**

* TLS 1.3 minimum version
* Perfect Forward Secrecy (PFS)
* HTTP Strict Transport Security (HSTS)
* Certificate pinning
* OCSP stapling

**API Communication:**

* All API endpoints require HTTPS
* Certificate validation
* Request/response encryption

3.2 Encryption at Rest

**Database Encryption:**

* AES-256 encryption for data at rest
* Encrypted database connections
* Encrypted backups

**Sensitive Data Encryption:**

// Column-level encryption for sensitive fields

const encrypt = (text: string): string => {

const algorithm = 'aes-256-gcm';

const iv = crypto.randomBytes(16);

const cipher = crypto.createCipheriv(algorithm, secretKey, iv);

let encrypted = cipher.update(text, 'utf8', 'hex');

encrypted += cipher.final('hex');

const authTag = cipher.getAuthTag();

return iv.toString('hex') + ':' + authTag.toString('hex') + ':' + encrypted;

};

**Encrypted Fields:**

* User passwords (bcrypt)
* API keys and secrets
* Personal identification numbers
* Financial data
* Two-factor authentication secrets

3.3 Key Management

**Encryption Key Hierarchy:**

* Master encryption key (environment variable)
* Data encryption keys (DEK)
* Key rotation policies (90-day cycle)
* Secure key storage

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. Input Validation & Sanitization

4.1 SQL Injection Prevention

**Parameterized Queries:**

// Safe database query pattern

const result = await pool.query(

'SELECT \* FROM users WHERE email = $1 AND organization\_id = $2',

[email, organizationId]

);

**Input Validation Middleware:**

* Whitelist validation for all inputs
* SQL pattern detection and blocking
* Parameterized query enforcement

4.2 Cross-Site Scripting (XSS) Prevention

**Output Encoding:**

* HTML entity encoding
* JavaScript escaping
* URL encoding
* CSS sanitization

**Content Security Policy (CSP):**

Content-Security-Policy:

default-src 'self';

script-src 'self' 'unsafe-inline';

style-src 'self' 'unsafe-inline' https://fonts.googleapis.com;

font-src 'self' https://fonts.gstatic.com;

img-src 'self' data: https: blob:;

connect-src 'self' https://onyx-backend-f7vh.onrender.com;

4.3 Cross-Site Request Forgery (CSRF) Protection

**CSRF Mitigation:**

* Origin header verification
* Referer header validation
* SameSite cookie attribute
* Double-submit cookie pattern

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5. Monitoring & Threat Detection

5.1 Security Event Logging

**Logged Events:**

* Authentication attempts (success/failure)
* Authorization violations
* Input validation failures
* Security header violations
* Suspicious behavior patterns
* Data access and modifications

**Log Structure:**

{

"timestamp": "2024-12-02T10:30:00Z",

"event\_type": "FAILED\_LOGIN",

"user\_id": "uuid",

"ip\_address": "192.168.1.100",

"user\_agent": "Mozilla/5.0...",

"details": {

"email": "user@example.com",

"failure\_reason": "invalid\_password",

"attempt\_count": 3

}

}

5.2 Real-Time Threat Detection

**Suspicious Activity Detection:**

* Multiple failed login attempts
* Unusual data access patterns
* Rapid API requests
* Geographic anomalies
* Time-based access anomalies
* Cross-organization data access

**Automated Response:**

* Account lockout
* IP blocking
* Rate limiting escalation
* Security team alerts

5.3 Security Metrics & KPIs

**Monitored Metrics:**

* Failed authentication attempts
* Security event frequency
* Response time to security incidents
* User security compliance rates
* Vulnerability detection and remediation time

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. API Security

6.1 Rate Limiting

**Rate Limiting Policies:**

// Authentication endpoints

authLimiter: {

windowMs: 15 \* 60 \* 1000, // 15 minutes

max: 5, // 5 attempts per window

skipSuccessfulRequests: true

}

// General API endpoints

apiLimiter: {

windowMs: 15 \* 60 \* 1000, // 15 minutes

max: 100, // 100 requests per window

skipSuccessfulRequests: false

}

6.2 API Key Management

**API Key Security:**

* 256-bit random key generation
* Scoped permissions
* Expiration dates
* Usage tracking
* Revocation capabilities

6.3 Request Validation

**Security Middleware Stack:**

1. Security context addition
2. SQL injection prevention
3. XSS protection
4. Parameter pollution prevention
5. Suspicious behavior detection
6. Origin verification

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. Infrastructure Security

7.1 Cloud Security (Render.com)

**Platform Security Features:**

* SOC 2 Type II compliant hosting
* Automatic security updates
* Network isolation
* DDoS protection
* Backup encryption
* Geographic redundancy

7.2 Container Security

**Security Measures:**

* Minimal base images
* Regular vulnerability scanning
* Secret management
* Resource limitations
* Network segmentation

7.3 Network Security

**Network Protection:**

* HTTPS enforcement
* TLS termination
* Network segmentation
* Firewall rules
* VPN access for administration

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. Compliance & Governance

8.1 Regulatory Compliance

**Standards Addressed:**

- **SOC 2 Type II**: Security, availability, processing integrity

- **GDPR**: Data protection and privacy rights

- **ISO 27001**: Information security management

- **NIST Cybersecurity Framework**: Identify, protect, detect, respond, recover

8.2 Data Governance

**Data Classification:**

- **Public**: Marketing materials, general documentation

- **Internal**: User guides, training materials

- **Confidential**: Assessment data, user information

- **Restricted**: Security configurations, encryption keys

**Data Retention Policies:**

* User data: Retained per legal requirements
* Security logs: 2-year retention
* Audit trails: 7-year retention
* Backup data: 30-day retention

8.3 Privacy Protection

**Privacy Measures:**

* Data minimization principles
* Purpose limitation
* Consent management
* Right to erasure (GDPR Article 17)
* Data portability
* Privacy by design

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9. Incident Response

9.1 Security Incident Response Plan

**Response Phases:**

1. **Preparation**: Team training, tools, procedures

2. **Detection**: Monitoring, alerting, analysis

3. **Containment**: Isolation, damage limitation

4. **Eradication**: Threat removal, vulnerability patching

5. **Recovery**: Service restoration, monitoring

6. **Lessons Learned**: Post-incident review, improvements

9.2 Incident Classification

**Severity Levels:**

- **Critical**: Active data breach, system compromise

- **High**: Attempted breach, significant vulnerability

- **Medium**: Security policy violation, suspicious activity

- **Low**: Minor security events, informational alerts

9.3 Communication Plan

**Stakeholder Notification:**

* Internal team: Immediate (0-1 hour)
* Management: High/Critical (1-4 hours)
* Customers: Critical incidents (4-24 hours)
* Regulators: As required by law

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10. Vulnerability Management

10.1 Vulnerability Assessment

**Assessment Methods:**

* Automated vulnerability scanning
* Manual penetration testing
* Code security reviews
* Dependency vulnerability checks
* Infrastructure assessments

10.2 Patch Management

**Patching Process:**

1. Vulnerability identification
2. Risk assessment
3. Patch testing (staging environment)
4. Change approval
5. Production deployment
6. Verification testing

**Patching Timeline:**

* Critical vulnerabilities: 24-48 hours
* High vulnerabilities: 7 days
* Medium vulnerabilities: 30 days
* Low vulnerabilities: 90 days

10.3 Security Testing

**Testing Types:**

- **SAST**: Static Application Security Testing

- **DAST**: Dynamic Application Security Testing

- **IAST**: Interactive Application Security Testing

- **Penetration Testing**: Quarterly external assessments

- **Red Team Exercises**: Annual comprehensive testing

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

11. Security Audit & Assessment

11.1 Automated Security Auditing

**Security Audit Service Features:**

// Automated security checks

const auditChecks = {

weakPasswords: 'Users with passwords not changed in 90+ days',

inactiveUsers: 'Users inactive for 30+ days',

failedLogins: 'Multiple failed login attempts',

suspiciousActivity: 'Unusual data access patterns',

dataIntegrity: 'Orphaned records and invalid data'

};

11.2 Compliance Auditing

**Audit Areas:**

* Access control effectiveness
* Data protection measures
* Security policy compliance
* Incident response procedures
* Vendor security assessments

11.3 Third-Party Assessments

**External Audits:**

* Annual penetration testing
* SOC 2 Type II audit
* ISO 27001 certification
* Vendor risk assessments

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

12. Business Continuity & Disaster Recovery

12.1 Backup Strategy

**Backup Implementation:**

* Automated daily backups
* Geographic redundancy
* Encrypted backup storage
* Regular restore testing
* Point-in-time recovery

12.2 Disaster Recovery Plan

**Recovery Objectives:**

- **RTO (Recovery Time Objective)**: 4 hours

- **RPO (Recovery Point Objective)**: 1 hour

- **Data Loss Tolerance**: < 15 minutes

12.3 Business Continuity

**Continuity Measures:**

* Multi-region deployment capability
* Load balancing and failover
* Database replication
* Communication plans
* Alternative work arrangements

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

13. Security Metrics & Reporting

13.1 Key Performance Indicators (KPIs)

**Security KPIs:**

* Mean Time to Detection (MTTD): < 5 minutes
* Mean Time to Response (MTTR): < 30 minutes
* Security incident frequency: Target < 1 per month
* Vulnerability remediation time: 95% within SLA
* User security training completion: 100%

13.2 Security Dashboard

**Dashboard Metrics:**

* Real-time threat alerts
* Failed authentication attempts
* System health status
* Vulnerability counts
* Compliance status

13.3 Executive Reporting

**Monthly Security Reports:**

* Security posture summary
* Incident summary
* Vulnerability status
* Compliance updates
* Risk assessment

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

14. Future Enhancements

14.1 Planned Security Improvements

**Short-term (3 months):**

* Zero Trust network architecture
* Advanced threat analytics
* Behavioral user analysis
* Enhanced encryption key management

**Medium-term (6 months):**

* AI-powered threat detection
* Automated incident response
* Advanced persistent threat (APT) protection
* Security orchestration and automated response (SOAR)

**Long-term (12 months):**

* Quantum-resistant cryptography preparation
* Advanced biometric authentication
* Blockchain-based audit trails
* Machine learning anomaly detection

14.2 Emerging Threat Preparation

**Threat Landscape Monitoring:**

* Zero-day vulnerability tracking
* Threat intelligence feeds
* Industry-specific threat analysis
* Regulatory change monitoring

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

15. Conclusion

The ONYX Platform security architecture represents a comprehensive, enterprise-grade security framework designed to protect against modern cybersecurity threats while maintaining operational efficiency and user experience. The multi-layered approach ensures robust protection of sensitive building assessment data and provides the foundation for regulatory compliance and business continuity.

Security Strengths

1. **Comprehensive Coverage**: End-to-end security from network to application layer

2. **Defense in Depth**: Multiple security barriers and controls

3. **Proactive Monitoring**: Real-time threat detection and response

4. **Compliance Ready**: Framework supports major compliance requirements

5. **Scalable Architecture**: Security measures scale with platform growth

Continuous Improvement

The security architecture is designed for continuous evolution, incorporating lessons learned from security assessments, threat landscape changes, and business requirements. Regular reviews and updates ensure the platform maintains its security posture against emerging threats.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Document Classification:** Confidential

**Next Review Date:** October 2025

**Document Owner:** ONYX Security Team

**Approval:** Chief Technology Officer

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\*This document contains confidential and proprietary information. Distribution is restricted to authorized personnel only.\*