next8n

SECURITY FRAMEWORK DIAGRAM

Workflow Automation Delivery Framework

ENTERPRISE EDITION

Version: 2.0

Date: December 28, 2025

Author: Mirza Iqbal

Contact: mirza.iqbal@next8n.com

Table of Contents

Security Framework Diagram

Complete Security Architecture for Workflow Automation Delivery

Security Layers Overview

```
flowchart TB
    subgraph LAYER1["LAYER 1: PERIMETER SECURITY"]
        L1A["HTTPS/TLS Encryption"]
        L1B["Domain Verification"]
        L1C["DDoS Protection"]
        L1D["Firewall Rules"]
    end

    subgraph LAYER2["LAYER 2: ACCESS CONTROL"]
        L2A["Role-Based Access (RBAC)"]
        L2B["Multi-Factor Authentication"]
        L2C["Session Management"]
        L2D["IP Whitelisting (optional)"]
    end

    subgraph LAYER3["LAYER 3: DATA PROTECTION"]
        L3A["Credential Encryption (AES-256)"]
        L3B["Runtime-Only Decryption"]
        L3C["Secure Memory Handling"]
        L3D["Data Minimization"]
    end

    subgraph LAYER4[" LAYER 4: WEBHOOK SECURITY"]
        L4A["Signature Verification"]
        L4B["Token Authentication"]
        L4C["Rate Limiting"]
        L4D["Payload Validation"]
    end

    subgraph LAYER5[" LAYER 5: COMPLIANCE"]
        L5A["GDPR Compliance"]
        L5B["Audit Logging"]
        L5C["Data Retention Policies"]
        L5D["Right to Deletion Support"]
    end

    LAYER1 --> LAYER2 --> LAYER3 --> LAYER4 --> LAYER5

    style LAYER1 fill:#ffebee
    style LAYER2 fill:#e8eaf6
    style LAYER3 fill:#e0f2f1
    style LAYER4 fill:#fff8e1
    style LAYER5 fill:#f3e5f5
```

Credential Security Architecture

```
flowchart TB
    subgraph CREATION[" Credential Creation"]
        CR1["Client signs up for service"]
        CR2["Client generates API key"]
        CR3["Key stored in client's vault"]
        CR4["One-time share link created"]
    end

    subgraph TRANSFER["Secure Transfer"]
        TR1["Share via encrypted channel"]
        TR2["Never via email/slack"]
        TR3["Use 1Password/Bitwarden links"]
        TR4["Link expires after use"]
    end

    subgraph STORAGE["n8n Storage"]
        ST1["Credential entered in n8n"]
        ST2["Encrypted with AES-256"]
        ST3["Stored in encrypted database"]
        ST4["Key never visible in UI"]
    end

    subgraph RUNTIME[" Runtime Use"]
        RU1["Workflow triggered"]
        RU2["Credential decrypted in memory"]
        RU3["API call made"]
        RU4["Credential cleared from memory"]
    end

    CREATION --> TRANSFER --> STORAGE --> RUNTIME

    style CREATION fill:#e3f2fd
    style TRANSFER fill:#fff3e0
    style STORAGE fill:#e8f5e9
    style RUNTIME fill:#f3e5f5
```

Webhook Hardening Architecture

```
flowchart TB
    subgraph INCOMING["Incoming Webhook"]
        INC1["External Service<br/>(Stripe, GitHub, etc.)"]
    end

    subgraph VALIDATION[" Validation Layer"]
        VAL1["Check HTTPS"]
        VAL2["Verify Signature"]
        VAL3["Validate Token"]
        VAL4["Check Rate Limit"]
        VAL5["Parse & Validate Payload"]
    end

    subgraph DECISION{" Valid?"}
    end

    subgraph ACCEPT[" Accept"]
        ACC1["Process webhook"]
        ACC2["Execute workflow"]
        ACC3["Log execution"]
    end

    subgraph REJECT[" Reject"]
        REJ1["Return 401/403"]
        REJ2["Log attempt"]
        REJ3["Alert if suspicious"]
    end

    INCOMING --> VALIDATION --> DECISION
    DECISION -->|"Yes"| ACCEPT
    DECISION -->|"No"| REJECT

    style VALIDATION fill:#fff3e0
    style ACCEPT fill:#e8f5e9
    style REJECT fill:#ffebee
```

Data Flow Security

```
flowchart LR
    subgraph SOURCE["Data Sources"]
        S1["CRM Data"]
        S2["Email Content"]
        S3["User Inputs"]
        S4["API Responses"]
    end

    subgraph CLASSIFY["Classification"]
        C1["PII Detection"]
        C2["Sensitivity Level"]
        C3["Retention Rules"]
    end

    subgraph PROCESS[" Processing"]
        P1["Data Minimization<br/>Only needed fields"]
        P2["Encryption in Transit<br/>TLS 1.3"]
        P3["Secure AI Processing<br/>No training on data"]
    end

    subgraph STORE["Storage"]
        ST1["Execution Logs<br/>Auto-prune enabled"]
        ST2["Error Logs<br/>Sensitive data redacted"]
        ST3["AI Logs<br/>For evaluation only"]
    end

    subgraph OUTPUT["Outputs"]
        O1["Actions taken"]
        O2["Notifications sent"]
        O3["Data stored"]
    end

    SOURCE --> CLASSIFY --> PROCESS --> STORE --> OUTPUT

    style CLASSIFY fill:#fff3e0
    style PROCESS fill:#e8f5e9
    style STORE fill:#e3f2fd
```

AI-Specific Security

```
flowchart TB
    subgraph AI_SECURITY[" AI Security Measures"]
        subgraph PROMPT["Prompt Security"]
            PR1["No secrets in prompts"]
            PR2["Prompt injection guards"]
            PR3["Output sanitization"]
        end

        subgraph DATA["Data Security"]
            DA1["No PII to AI unless required"]
            DA2["Use anonymized data when possible"]
            DA3["Clear data retention policies"]
        end

        subgraph MODEL["Model Selection"]
            MO1["Prefer privacy-first models"]
            MO2["Consider self-hosted LLMs"]
            MO3["Verify data handling policies"]
        end

        subgraph OUTPUT["Output Safety"]
            OU1["Content filtering"]
            OU2["Tone verification"]
            OU3["Jailbreak prevention"]
        end
    end

    style AI_SECURITY fill:#f3e5f5
```

Compliance Architecture (GDPR Focus)

```
flowchart TB
    subgraph GDPR[" GDPR Compliance Requirements"]
        subgraph LAWFUL["Lawful Basis"]
            LB1["Client has consent/contract"]
            LB2["Processing is documented"]
            LB3["Purpose is specified"]
        end

        subgraph RIGHTS["Data Subject Rights"]
            DR1["Right to Access"]
            DR2["Right to Rectification"]
            DR3["Right to Erasure"]
            DR4["Right to Portability"]
        end

        subgraph PROTECTION["Data Protection"]
            DP1["Encryption at rest"]
            DP2["Encryption in transit"]
            DP3["Access controls"]
            DP4["Audit logging"]
        end

        subgraph BREACH["Breach Handling"]
            BR1["Detection system"]
            BR2["72-hour notification"]
            BR3["Documentation"]
            BR4["Remediation"]
        end
    end

    subgraph IMPLEMENTATION[" Implementation"]
        IMP1["Data Processing Agreement<br/>with client"]
        IMP2["Retention policies<br/>configured in n8n"]
        IMP3["Deletion workflows<br/>if needed"]
        IMP4["Audit trail<br/>maintained"]
    end

    GDPR --> IMPLEMENTATION
```

Access Control Matrix

```
flowchart TB
    subgraph ROLES["Roles"]
        OWNER["Owner<br/>Full control"]
        ADMIN["Admin<br/>Manage users"]
        EDITOR["Editor<br/>Build workflows"]
        VIEWER["Viewer<br/>Read only"]
    end

    subgraph PERMISSIONS["Permissions"]
        subgraph WORKFLOW["Workflows"]
            W_CREATE["Create"]
            W_EDIT["Edit"]
            W_DELETE["Delete"]
            W_EXECUTE["Execute"]
            W_VIEW["View"]
        end

        subgraph CREDS["Credentials"]
            C_CREATE["Create"]
            C_USE["Use"]
            C_VIEW["View Values"]
            C_DELETE["Delete"]
        end

        subgraph USERS["Users"]
            U_INVITE["Invite"]
            U_REMOVE["Remove"]
            U_ROLES["Change Roles"]
        end
    end

    OWNER --> W_CREATE & W_EDIT & W_DELETE & W_EXECUTE & W_VIEW
    OWNER --> C_CREATE & C_USE & C_VIEW & C_DELETE
    OWNER --> U_INVITE & U_REMOVE & U_ROLES

    ADMIN --> W_CREATE & W_EDIT & W_DELETE & W_EXECUTE & W_VIEW
    ADMIN --> C_CREATE & C_USE
    ADMIN --> U_INVITE

    EDITOR --> W_CREATE & W_EDIT & W_EXECUTE & W_VIEW
    EDITOR --> C_USE

    VIEWER --> W_VIEW
```

Security Incident Response

```
flowchart TB
    subgraph DETECT[" Detection"]
        D1["Unusual execution patterns"]
        D2["Failed auth attempts"]
        D3["Unexpected data access"]
        D4["Error spikes"]
    end

    subgraph ASSESS[" Assessment"]
        A1["Identify scope"]
        A2["Classify severity"]
        A3["Document timeline"]
    end

    subgraph CONTAIN["Containment"]
        C1["Disable affected workflows"]
        C2["Revoke credentials"]
        C3["Block suspicious IPs"]
    end

    subgraph NOTIFY["Notification"]
        N1["Alert internal team"]
        N2["Notify client if needed"]
        N3["Regulatory notification<br/>(if required)"]
    end

    subgraph RECOVER[" Recovery"]
        R1["Fix vulnerability"]
        R2["Restore from backup"]
        R3["Re-enable systems"]
        R4["Post-mortem"]
    end

    DETECT --> ASSESS --> CONTAIN --> NOTIFY --> RECOVER

    style DETECT fill:#ffebee
    style CONTAIN fill:#fff3e0
    style RECOVER fill:#e8f5e9
```

Security Checklist Summary

CATEGORY	REQUIREMENT	PRIORITY
Transport	HTTPS only	Critical
Credentials	Encrypted at rest	Critical
Webhooks	Signature verification	High
Access	RBAC configured	High
Logging	Audit trail enabled	High
Data	Minimization practiced	Medium
Compliance	DPA in place	Medium
AI	Prompt injection guards	Medium

Next: See `05-handover-process.md` for delivery workflow details.