

Security Architecture

Version: 1.0.0 **Date:** 2026-07-07

Introduction

Introduction

This document describes the technical and organisational security measures implemented by Evidia to protect the Evidia Platform (the “Service”) and customer data.

Security is a foundational principle of our platform design. We implement defence-in-depth strategies, zero-trust principles, and continuous monitoring to protect against threats.

Security Governance

Security Governance

Security Leadership

- Security oversight is provided by senior leadership
- Security responsibilities are defined for all personnel
- Regular security training is mandatory for all staff

Security Policies

We maintain documented policies covering:

1. Information security policy
2. Access control policy
3. Data classification policy
4. Incident response policy
5. Business continuity policy
6. Vendor management policy

Compliance Framework

Our security controls align with:

- ISO/IEC 27001 control framework
- EU AI Act security requirements
- GDPR security requirements
- Industry best practices

Infrastructure Security

Infrastructure Security

Hosting Environment

Component	Details
Cloud provider	Hetzner
Region	European Union (EU-only)
Network isolation	Virtual private cloud with restricted access
Load balancing	Application-level load balancing
Container security	Docker containers with minimal attack surface

Network Security

Network Architecture

1. Private network with controlled ingress/egress
2. Firewall rules restricting traffic to necessary ports
3. TLS termination at the application layer
4. No direct database access from public networks

DDoS Protection

1. Rate limiting on API endpoints
2. Traffic analysis and anomaly detection
3. Graceful degradation under attack

Server Hardening

1. Minimal base images with regular security updates
2. Unnecessary services and packages removed
3. Host-based firewalls
4. Regular vulnerability scanning

Data Security

Data Security

Data Classification

Classification	Examples	Handling
Confidential	Audio, transcripts, PII	Encrypted, access-controlled

Classification	Examples	Handling
Internal	Configuration, logs	Access-controlled
Public	Marketing content	Standard handling

Encryption

Encryption at Rest

- **Algorithm:** AES-256
- **Scope:** All stored data including databases, object storage, and backups
- **Key management:** Secure key storage with regular rotation

Encryption in Transit

- **Protocol:** TLS 1.3
- **Scope:** All network communications
- **Certificate management:** Automated certificate renewal

Secrets Management

- **Approach:** Self-hosted secrets management infrastructure
- **Scope:** API keys, database credentials, encryption keys
- **Practices:** Secrets never logged, rotated regularly, least-privilege access

Data Residency

- All customer data is stored and processed within the European Union
- No cross-border data transfers without explicit consent
- Sub-processors verified for EU data residency

Data Retention and Deletion

Data Type	Retention	Deletion Method
Audio recordings	Tenant-configurable	Secure deletion from object storage
Transcripts	Tenant-configurable	Database record deletion
Consent records	Tenant-configurable, subject to applicable legal requirements	Database record deletion

Data Type	Retention	Deletion Method
Audit logs	Tenant-configurable, subject to security and compliance requirements	Anonymisation then deletion
Account data	Until request	Full account deletion

Access Control

Access Control

Authentication

User Authentication

- **Method:** OpenID Connect (OIDC)
- **Providers:** OpenID Connect (Google, Microsoft 365)
- **MFA:** Multi-factor authentication available and recommended
- **Session management:** Secure session tokens with automatic expiration

Service Authentication

- Internal service-to-service authentication
- API key rotation for external integrations
- Mutual TLS for sensitive internal communications

Authorisation

Role-Based Access Control (RBAC)

Role	Permissions
Owner	Full organisation management, billing, user management
Admin	User management, settings, integrations
Member	Meeting access, analysis review
Viewer	Read-only access to assigned meetings

Row-Level Security (RLS)

We implement database-level row-level security for multi-tenant isolation:

1. All tenant-scoped tables have RLS enabled
2. RLS policies enforce `app.current_tenant_id` filtering

3. Session-scoped database context prevents cross-tenant access
4. Defence-in-depth: application queries also include explicit tenant filters

Principle of Least Privilege

1. Users granted minimum permissions necessary
2. Regular access reviews and certification
3. Time-limited elevated access where required

Administrative Access

1. Separate administrative accounts
2. MFA required for all administrative access
3. All administrative actions logged
4. Break-glass procedures for emergency access

Application Security

Application Security

Secure Development

Development Practices

1. Secure coding guidelines and training
2. Code review required for all changes
3. Automated security scanning in CI/CD pipeline
4. Dependency vulnerability monitoring

Security Testing

1. Static application security testing (SAST)
2. Dynamic application security testing (DAST)
3. Dependency vulnerability scanning
4. Periodic penetration testing

Input Validation

1. All user input validated and sanitised
2. Parameterised queries prevent SQL injection
3. Output encoding prevents XSS attacks
4. File upload validation and scanning

API Security

1. Rate limiting on all endpoints
2. Authentication required for protected endpoints
3. Input validation on all parameters
4. CORS policies restrict cross-origin requests
5. Content Security Policy (CSP) headers

Webhook Security

1. HMAC-SHA256 signature verification
2. Timestamp validation to prevent replay attacks
3. Idempotency keys for deduplication
4. Secure endpoint URLs

Audit Logging

Audit Logging

Audit Trail Architecture

We maintain comprehensive audit logging with integrity measures:

1. **Event chaining:** Audit events are linked to enable integrity verification
2. **Comprehensive coverage:** Security-relevant events are logged
3. **Append-only storage:** Audit logs cannot be modified after creation

Logged Events

Authentication Events

- Login success/failure
- Logout
- Session creation/revocation
- MFA enrolment/removal

Authorisation Events

- Role grants/revocations
- Permission changes
- API key creation/rotation/revocation
- Policy changes

Data Access Events

- Transcript viewed
- Audio downloaded
- Report exported
- Data exports

AI System Events

- AI inference requested/completed
- Human approval granted/denied
- AI output overridden
- Quality issues reported

Administrative Events

- Configuration changes
- Integration setup/modification
- Security setting changes

Audit Log Protection

1. Logs stored separately from application data
2. Access restricted to authorised personnel
3. Log access itself is audited
4. Retained for Tenant-configurable, subject to security and compliance requirements

Monitoring and Detection

Monitoring and Detection

Infrastructure Monitoring

1. Real-time metrics collection
2. Resource utilisation monitoring
3. Automated alerting for anomalies
4. Centralised log aggregation

Security Monitoring

1. Failed authentication attempt monitoring
2. Unusual access pattern detection
3. Privilege escalation monitoring
4. Data exfiltration detection

Distributed Tracing

1. OpenTelemetry-based distributed tracing
2. Request correlation across services
3. Performance monitoring
4. Error tracking and alerting

Alerting

1. 24/7 monitoring and alerting
2. Severity-based escalation procedures
3. On-call rotation for critical alerts
4. Regular alert review and tuning

Incident Response

Incident Response

Incident Classification

Severity	Examples	Response Time
Critical	Data breach, system compromise	Immediate
High	Security vulnerability, outage	1 hour
Medium	Performance degradation, errors	4 hours
Low	Minor issues, cosmetic bugs	24 hours

Response Process

1. **Detection:** Automated monitoring or user report
2. **Triage:** Severity assessment and team notification
3. **Containment:** Isolate affected systems
4. **Eradication:** Remove threat and patch vulnerabilities
5. **Recovery:** Restore services and verify integrity
6. **Post-incident:** Root cause analysis and documentation

Communication

1. Internal stakeholders notified per severity
2. Affected customers notified without undue delay
3. Regulatory notification within 72 hours where required
4. Post-incident report provided to affected parties

Business Continuity

Business Continuity

Backup Strategy

1. Regular automated backups of all data
2. Encrypted backup storage
3. Off-site backup replication
4. Regular backup restoration testing

Disaster Recovery

1. Documented disaster recovery procedures
2. Recovery time objective (RTO): **[TODO: RTO]**
3. Recovery point objective (RPO): **[TODO: RPO]**
4. Regular disaster recovery testing

High Availability

1. Redundant infrastructure components
2. Automatic failover for critical services
3. Load balancing across multiple instances
4. Geographic redundancy where applicable

Vendor Security

Vendor Security

Vendor Assessment

Before engaging vendors, we assess:

1. Security certifications and practices
2. Data processing locations
3. Compliance with relevant regulations
4. Incident response capabilities

Vendor Requirements

All vendors processing customer data must:

1. Sign data processing agreements
2. Maintain appropriate security controls
3. Process data only within the EU
4. Notify us of security incidents

Ongoing Monitoring

1. Regular vendor security reviews
2. Monitoring of vendor security announcements
3. Contractual right to audit

Physical Security

Physical Security

Data Centre Security

Our cloud provider (Hetzner) maintains physical security including:

1. 24/7 security personnel and surveillance
2. Biometric access controls
3. Environmental controls (fire, flood, temperature)
4. Uninterruptible power supply and generators

Office Security

1. Physical access controls
2. Clean desk policy
3. Secure disposal of physical media

Security Certifications

Security Certifications

[TODO: List current security certifications, e.g.:]

- ISO/IEC 27001:2013 (planned)
- SOC 2 Type II (planned)

Contact

Security Contact

For security concerns or to report a vulnerability:

- **Security team:** security@evidia.ai
- **Responsible disclosure:** We appreciate responsible disclosure of security vulnerabilities