Security Whitepaper

Last updated: 9 June 2026

1. INTRODUCTION

Opisense is an AI-powered business platform combining an intelligent workspace, AI agents, and integration capabilities to help companies manage and automate their operations. This whitepaper describes the security architecture, practices, and compliance posture of the Opisense platform.

2. COMPLIANCE AND CERTIFICATIONS

Opisense is implementing an Information Security Management System (ISMS) aligned with ISO 27001:2022 standards. Third-party certification audits are scheduled for H2-H3 2026. Current compliance status:

- GDPR: Fully compliant. Data Processing Agreement available at opisense.com/legal.
- EU AI Act: Aligned with transparency and human oversight requirements for AI systems.
- NIS2 (Network and Information Security Directive 2): Security measures and incident reporting framework in place.
- ISO 27001:2022 ISMS: Framework and controls under implementation. Independent certification audit scheduled H3-H4 2026. Certification status: Pending.
- SOC 2 Type II: Readiness evaluation underway. Formal audit engagement targeted for H3-H4 2026 to complete Type II report by H4 2026.

Opisense is registered with the Norwegian Data Protection Authority (Datatilsynet) and operates under Norwegian and EU data protection law. The ISMS encompasses access controls, encryption, incident response, vulnerability management, and personnel security as detailed in subsequent sections.

3. INFRASTRUCTURE AND HOSTING

The platform is hosted on Hetzner cloud infrastructure in the European Union (data centres in Germany and Finland). Application delivery is handled through Vercel's edge network. Backend data infrastructure runs on Convex and Supabase. Hetzner operates ISO 27001-certified, GDPR-compliant EU data centres. Opisense leverages network isolation, firewall security groups, and automated patching.

4. DATA ENCRYPTION

IN TRANSIT

All data transmitted between users, the platform, and integrated services is encrypted using TLS 1.2 minimum (TLS 1.3 preferred).

AT REST

All stored data is encrypted using AES-256 encryption.

KEY MANAGEMENT

Encryption keys are managed through a dedicated key management service with automatic key rotation.

5. ACCESS CONTROL

- Role-based access control (RBAC) is enforced across the platform.
- Multi-factor authentication (MFA) is available for all user accounts.
- Administrative access to production systems is restricted, logged, and reviewed.
- Least-privilege principles are applied to all system and service accounts.
- User authentication is managed through Clerk with session management and token-based access.
- Platform activity is monitored through Axiom for security event detection and anomaly alerting.

These mechanisms ensure comprehensive access management and security monitoring.

6. AI MODEL SECURITY

The platform integrates with third-party AI model providers through API connections with zero-data-retention configurations. Models from OpenAI, Anthropic, Google, Mistral, xAI, Groq, Perplexity, DeepSeek, Alibaba, Moonshot and Zhipu are accessed via the OpenRouter gateway with EU in-region routing enabled, among other vetted AI service providers.

- Customer data is not used to train third-party AI models.
- AI model outputs are clearly identified as AI-generated within the platform.
- The platform enforces content filtering and safety boundaries on AI interactions.

Voice processing, including speech-to-text and text-to-speech, is provided through Elevenlabs under zero-retention API terms.

7. APPLICATION SECURITY

- Secure development lifecycle (SDLC) practices are followed.
- Code reviews are required for all production changes.
- Dependency scanning is performed to identify known vulnerabilities.
- Web application firewall (WAF) protects against common attack vectors.

8. SECURITY TESTING PROGRAMME

Opisense maintains a multi-layered security testing programme to validate the effectiveness of technical and organisational controls:

INTERNAL SECURITY TESTING (OPERATIONAL NOW)

- **Code Review Process:** All production code changes undergo mandatory peer review via pull requests (PR) to identify security flaws, logic errors, and architectural issues before deployment.
- **Dependency Scanning:** Continuous scanning via solutions such as Dependabot and Snyk identifies vulnerable dependencies in application and infrastructure code, with automated alerts and remediation tracking.
- **Container Scanning:** For example, Docker images and container artifacts are scanned for known vulnerabilities before deployment to production.
- **Static Application Security Testing (SAST):** Automated code analysis detects common security vulnerabilities including injection flaws, weak cryptography, and authentication bypasses.
- **Dynamic Application Security Testing (DAST):** Black-box application testing simulates real-world attack scenarios against running services.
- **Quarterly Vulnerability Assessments:** Comprehensive internal security assessments identify misconfigurations, unpatched systems, and control weaknesses across the infrastructure.

EXTERNAL SECURITY TESTING (VALIDATION LAYER)

To complement internal testing and provide independent validation, Opisense engages reputable third-party security firms for external penetration testing. The first external penetration test is scheduled for completion by end of Q4 2026, in parallell with ISO 27001 certification audit in H4 2026. Annual external penetration testing is planned to evaluate and enhance the effectiveness of security controls.

This testing pyramid, unit testing, integration testing, security testing, and external penetration testing ensures comprehensive security validation from development through production. The external penetration tests serves as an independent capstone validation that supplements the continuous internal testing programme.

9. VULNERABILITY MANAGEMENT

Opisense maintains a defined vulnerability management process with severity-based Service Level Agreements (SLAs) for detection, response, and remediation:

Severity Level	Detection & Response SLA	Remediation SLA
Critical	24 hours	3 days
High	48 hours	7 days
Medium	5 business days	30 days
Low	30 days	60 days

Critical vulnerabilities are immediately triaged and escalated to the security team. A patch or mitigation is deployed within 72 hours, or a risk acceptance is formally documented.

High severity vulnerabilities are addressed within 7 days with priority scheduling.

Medium and Low severity vulnerabilities are remediated within standard maintenance windows and follow routine patching schedules.

All vulnerability findings are logged, tracked, and subject to evidence of remediation before closure. Vulnerability reports are reviewed monthly by the security team.

10. RISK MANAGEMENT

- Opisense maintains a risk register reviewed quarterly.
- Risk assessments are conducted for new features, integrations, and sub-processors.
- Data Protection Impact Assessments (DPIAs) are performed where required by GDPR.

11. OPERATIONS SECURITY

LOGGING AND MONITORING

Platform activity is logged through Axiom and monitored for security events.

INCIDENT RESPONSE

Documented incident response procedures with defined escalation paths and 48-hour breach notification requirements.

BACKUP AND RECOVERY

Regular automated backups with Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of 24 hours each.

CHANGE MANAGEMENT

All production changes follow documented approval processes.

12. PERSONNEL SECURITY

- All Opisense employees are subject to background verification appropriate to their role.
- Security awareness training is provided to all personnel.
- Access is revoked immediately upon termination of employment.

13. SUB-PROCESSOR MANAGEMENT

The platform relies on a comprehensive list of sub-processors for infrastructure and hosting, AI inference and gateway services, authentication, payments, agent web browsing and code execution, integrations, email delivery, and observability. This expanded provider list ensures service coverage and redundancy.

- All sub-processors are subject to security assessment before engagement.
- Sub-processor agreements include data protection and security requirements, including Standard Contractual Clauses for transfers outside the EU/EEA.
- A current list of sub-processors is maintained at opisense.com/legal/subprocessor-register-opisense.
- Customers receive 30 days' notice before new sub-processors are engaged.
- Transfer impact assessments are conducted for each sub-processor and reviewed when material changes occur.

14. BUSINESS CONTINUITY

- Opisense maintains business continuity and disaster recovery plans.
- Recovery objectives: RTO 24 hours, RPO 24 hours.
- Plans are reviewed and tested annually.

15. DATA RETENTION AND DELETION

Customer data handling upon contract termination follows the Data Processing Agreement:

- Customer has 30 days to export data in machine-readable format (JSON, CSV, etc.)
- Opisense completes deletion of remaining data within 60 days of termination

This is a sequential timeline: Customer receives a 30-day export window, followed by Opisense completing deletion by day 60. Voice data is automatically deleted after 7 days unless the Customer opts for longer retention.

16. FREQUENTLY ASKED QUESTIONS

Q: WHERE IS MY DATA STORED?

A: Customer data is stored on Hetzner infrastructure in the EU (data centres in Germany and Finland). Some processing occurs through US-based sub-processors under Standard Contractual Clauses and, where applicable, the EU-US Data Privacy Framework.

Q: IS MY DATA USED TO TRAIN AI MODELS?

A: No. Customer data is never used to train AI models. Opisense enforces zero-data-retention policies with AI providers including OpenAI, Anthropic and more.

Q: WHICH AI PROVIDERS DOES OPISENSE USE?

A: The platform integrates with OpenAI, Anthropic, Google, Perplexity, xAI, Groq, Mistral, DeepSeek, OpenRouter, Alibaba, Moonshot and Zhipu for AI model inference, and Elevenlabs for voice processing. All operate under zero-data-retention API configurations.

Q: WHAT HAPPENS TO MY DATA AFTER CONTRACT TERMINATION?

A: Following your written request, you have 30 days to export your data, and Opisense deletes remaining data within 60 days of contract termination. See Section 15 for details.

Q: HOW DO I REPORT A SECURITY CONCERN?

A: Contact security@opisense.com or your account representative.

Q: CAN I REQUEST A PENETRATION TEST REPORT?

A: Yes. Contact security@opisense.com for the latest report summary.