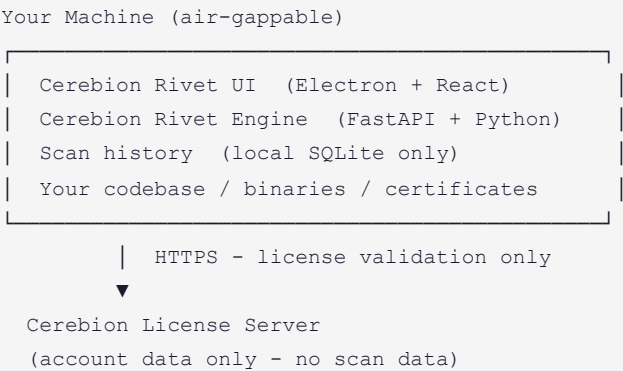


Cerebion Rivet is a **desktop application that runs entirely on your infrastructure**. Your source code, binaries, certificates, and scan results never leave your machine. Cerebion LLC does not operate a cloud scanning service and does not receive, process, or store any of your intellectual property.

The only exception: if you choose to configure the optional AI features (fix recommendations and report generation), data is sent directly from your machine to your chosen AI provider (Google, Anthropic, OpenAI, or a self-hosted local model) - never to Cerebion. For complete air-gap operation, use a local model such as Ollama - no data leaves your machine at all. These features are **off by default** and require explicit configuration to enable.

1. Architecture Overview



- ✓ Standard desktop app - no kernel drivers, no system services
- ✓ Does not intercept or monitor network traffic
- ✓ AI features (fix + report generation) off by default - requires your own API key
- ✓ No administrator/root privileges required to install or run
- ✓ Does not modify source code without explicit user action
- ✓ 7-day offline license cache - air-gap deployments supported

2. Data Handling

What Stays on Your Machine (Always)

Data	Location	Transmitted to Cerebion?
Source code files	Your filesystem	Never
Binaries scanned	Your filesystem	Never
TLS certificates analyzed	Your machine	Never
Scan findings and reports	Local SQLite DB	Never
Network scan results	Local SQLite DB	Never

What Is Transmitted (License Validation Only)

Data	Destination	Purpose	Frequency
License key	Cerebion License Server	Validate active license	On startup, cached 7 days
Device fingerprint	Cerebion License Server	Enforce seat count	On startup
Account email	Cerebion License Server	Account identity	On login only

AI Features (Optional - Off by Default)

There are two AI data flows, both optional and user-initiated:

AI Fix Generation - Triggered when you request a fix for a specific finding - Sends the relevant code snippet to your chosen AI provider	AI Report Generation - Triggered when you select findings and request an AI report - Sends selected finding metadata (algorithm names, severities, file paths) to your chosen AI provider
--	---

Provider	Type	Data Leaves Machine?
Google Gemini	Cloud (your API key)	Yes - to Google only
Anthropic Claude	Cloud (your API key)	Yes - to Anthropic only
OpenAI GPT	Cloud (your API key)	Yes - to OpenAI only
Ollama / LM Studio	Local / on-premise	No - stays on your machine
Any OpenAI-compatible endpoint	Self-hosted / private cloud	Depends on your endpoint

How it works - Your API key stored locally in Electron encrypted store - Data sent directly to your chosen provider — never to Cerebion - Only content you explicitly select is included - AI is for fixes and reports only - not detection	Maximum data privacy - Use Ollama or LM Studio for fully local AI - No data leaves your machine at all - Or simply don't configure AI - all rule-based scanning works without it
---	--

3. Security Controls

Code Signing and Integrity

Platform	Method	Certificate Authority	Verification
Windows	EV Code Signing	DigiCert	Right-click installer → Digital Signatures → "Cerebion LLC"
macOS	Apple Notarization	Apple	Gatekeeper validates automatically
Linux	SHA-256 checksum	-	Verify against hash published at cerebion.com/download

SBOM Available Format: CycloneDX JSON	Dependency Audit - v1.1.73 Python: 0 CVEs in shipped code
---	---

- Lists all bundled dependencies + versions
 - Per-platform (Windows, Linux, macOS)
 - Available on request: support@cerebion.com
- Node.js: 0 vulnerabilities
 - Tool: pip-audit + npm audit
 - Run before every release

No Telemetry

Cerebion Rivet does not collect usage analytics, crash reports, feature statistics, keystrokes, or clipboard data. All scan data is stored locally at %APPDATA%\CerebionRivet\ (Windows), ~/Library/Application Support/CerebionRivet/ (macOS), or ~/.config/CerebionRivet/ (Linux). You own this data. Uninstalling removes it.

4. Permissions and System Access

- What Cerebion Rivet Accesses

 - Read files in the folder you select
 - Read binary files you specify
 - Network: license.cerebion.com:443 (license)
 - Network: AI provider (only if you configure it)
 - Local disk write to app data folder
- What It Does NOT Access

 - Files outside your selected folder
 - Other processes or applications
 - Network traffic or packet capture
 - Credential stores or password managers
 - Camera, microphone, or peripherals

5. Infrastructure Security (License Server)

Control	Implementation
Transport encryption	TLS 1.2+ enforced, no downgrade
Authentication	JWT tokens (short-lived)
Data at rest	PostgreSQL on EC2, localhost only - not internet-exposed
DDoS protection	AWS CloudFront WAF
AWS certifications	SOC 1/2/3, ISO 27001, PCI DSS Level 1
Account data held	Email address, hashed password, license key, device fingerprint

6. Cryptographic Standards

Use Case	Algorithm	Standard
License authentication	JWT HS256	RFC 7519
Offline license signing	Ed25519	RFC 8032
Transport security	TLS 1.2 / 1.3	RFC 8446
Local credential storage	Electron safeStorage (AES)	Platform keychain
Password hashing (server)	bcrypt (cost 12)	-

We are evaluating migration to ML-KEM (FIPS 203) for license communication in a future release, consistent with our product's own recommendations for customers.

7. Compliance Posture

SOC 2 Not applicable - Cerebion does not process or store customer scan data	PCI DSS Not applicable - no payment data handled by Cerebion Rivet	GDPR License server holds account email only. Data deletion available on request.
HIPAA Cerebion Rivet does not handle PHI	FedRAMP Not certified - contact us for federal deployment discussion	Air-Gap Supported - 7-day offline cache. Enterprise air-gap licensing available on request.

8. Enterprise Deployment

Deployment • Standard per-user or per-machine installer • Compatible with SCCM, Intune, Jamf, Ansible • No special runtime privileges required • Deploy from cerebion.com/download only	Network Allowlist • license.cerebion.com:443 - required (or 7-day offline) • generativelanguage.googleapis.com:443 - optional (Gemini) • api.anthropic.com:443 - optional (Claude) • api.openai.com:443 - optional (OpenAI) • localhost or internal URL - optional (local model)
---	---

9. Vulnerability Disclosure

Report vulnerabilities to **support@cerebion.com**. We acknowledge within 24 hours and provide a fix timeline within 48 hours. We do not pursue legal action against good-faith security researchers.

10. Contact

Security Questions & Vulnerability Reports support@cerebion.com	Enterprise Deployment Support support@cerebion.com
SBOM Requests support@cerebion.com	General Support support@cerebion.com

This document is provided for informational purposes only and does not constitute a warranty, guarantee, or contractual commitment. See your Cerebion License Agreement for binding terms.