CONFIDENTIAL

CEO JUICE

MCP Platform

Security & Data Handling

For Dealer IT & Security Review

Version 1.0 | April 2026

Prepared by CEOJuice Solutions Architecture

This document describes the security architecture, data handling practices, and tenant isolation model for the CEOJuice MCP intelligence platform.

Contents

1. Executive Summary 3

2. Architecture Overview 4

3. Data Flow & Handling 5

4. Network Security 7

5. Tenant Isolation 8

6. Authentication & Access Control 9

7. AI / LLM Security 10

8. Memory Layer 11

9. Data Retention & Deletion 13

10. Incident Response & Availability 14

11. Operational Security 15

Appendix A: Technical Specifications 17

Appendix B: Compliance & Certifications 18

Appendix C: FAQ for IT Teams 19

1. Executive Summary

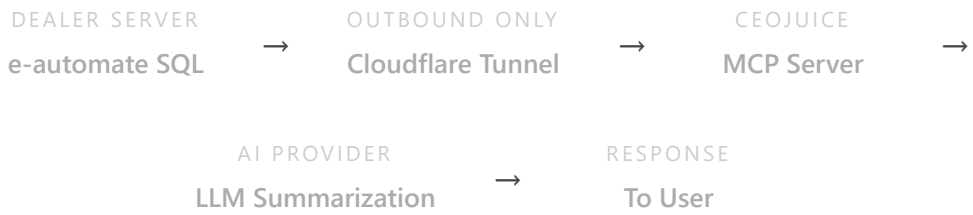
The CEOJuice MCP platform provides AI-powered business intelligence for e-automate. Dealers ask questions about their business data in plain language and receive intelligent, contextual answers. The platform is built on CEOJuice's 20-year library of e-automate process logic and learns each dealer's operational patterns over time.

Security Commitments

- **Controlled database access.** At launch, the platform queries your e-automate SQL Server with read-only (SELECT) permissions. Future write capabilities will only be introduced with explicit dealer approval and are always governed by permissions your DBA controls.
- **No bulk business data stored.** Query results (financial figures, customer records, invoice details) are processed in-memory and not persisted to any application-level storage on CEOJuice infrastructure.
- **Encrypted end-to-end.** All data in transit is protected by TLS 1.3 via Cloudflare Tunnel. Data at rest in the memory layer is encrypted with AES-256.
- **Per-dealer tenant isolation.** Each dealer has a physically separate data path (own SQL Server, own tunnel). The memory layer is scoped to your tenant and inaccessible to other dealers.
- **LLM provider with zero-retention policy.** The AI model that generates responses does not retain your data beyond the request lifecycle and does not use it for model training.
- **Full data export and deletion on request.** You can request a complete export of your memory layer data or full deletion at any time.

> **If you have approved CEO Juice Core, the MCP platform uses the same trust model with additional protections.** CEO Juice Core has read/write SQL access and interactive remote sessions. MCP launches with read-only access, no interactive sessions, and multi-layer query validation. This is not a new trust relationship. It is a more constrained version of the trust you have already extended.

2. Architecture Overview



What Lives Where

LOCATION	COMPONENTS	DATA
Dealer Server	e-automate SQL Server, CEO Juice Core, Cloudflare tunnel daemon	All business data remains here. Nothing moves unless queried.
Cloudflare	TLS termination, Zero Trust access control, tunnel routing	Encrypted transit only. No data stored.
CEOJuice Infrastructure	MCP server, memory layer (PostgreSQL, Neo4j, cache)	Telemetry metadata and memory layer (Section 8). No raw business data.
LLM Provider	AI model for response generation	Receives query results for summarization. Zero retention per API policy.

Query results transit from the dealer's SQL Server through the Cloudflare tunnel to the MCP server, where they are processed in-memory, sent to the LLM provider for summarization, and returned to the user. Results are not retained after the response is delivered and are not persisted to any application-level storage, log, or database on CEOJuice infrastructure.

3. Data Flow & Handling

Database Access

At launch, the MCP server connects to your e-automate SQL Server using a dedicated read-only account with SELECT-only permissions. The platform answers questions and surfaces insights but cannot modify any data.

Future capabilities may include the ability to take actions on your behalf (e.g., updating a record or creating an entry). Any such capability will require your explicit approval and will be governed by database permissions your DBA controls. No permission escalation happens without your DBA's action.

Your DBA retains full control over the MCP account at all times. Permissions are verifiable on your SQL Server, and you can revoke access immediately by disabling the account.

Query Validation (Defense in Depth)

Multiple independent layers govern all database interactions:

LAYER	CONTROL	WHAT IT PREVENTS
1. Database	SQL account permissions set by dealer's DBA. At launch: SELECT-only grants. No EXECUTE, CREATE, ALTER, or DROP permissions. Any future permission changes require the DBA's action.	Any action beyond what the DBA has explicitly permitted.
2. Application	Query validator blocks unauthorized operations using word-boundary pattern matching. Blocks SQL injection patterns: semicolons, comment markers (--), and system procedure prefixes (xp_, sp_).	SQL injection, statement chaining, unauthorized operations.
3. Tool	Pre-built tools use hardcoded, parameterized queries. The AI model provides parameter values but cannot modify query structure.	AI-generated queries that deviate from intended patterns.
4. Audit	Every tool call is logged with timestamp, tool identifier, and success/error status. Logs contain operational metadata only — not raw SQL text or	Undetected or unaccountable data access.

LAYER	CONTROL	WHAT IT PREVENTS
	query results. Dealers can request audit logs at any time.	

> **Custom query tool:** The platform includes an analytical tool that accepts flexible SELECT statements for ad-hoc analysis. These queries pass through all layers above: database permissions constrain accessible tables, the query validator blocks dangerous patterns, and every execution is logged (tool identifier, timestamp, success/error — not the raw SQL text).

What IS Stored on CEOJuice Infrastructure

- **Tool call metadata:** Process ID, timestamp, success or error status, token count. This is operational telemetry. It does not contain business data (no dollar amounts, no customer names, no query results).
- **Memory layer:** Operational patterns, schema facts, and session context that enable the system to improve over time. Described in detail in Section 8.

What is NOT Stored

- Raw query result sets
- Financial figures (revenue, costs, balances, invoice amounts)
- Customer records or personally identifiable information
- Invoice details, payment records, or transaction data

4. Network Security

Cloudflare Tunnel

The connection between your server and CEOJuice uses a Cloudflare Tunnel. This is an outbound-only connection initiated from your server. No inbound ports are opened. No firewall rules are changed. No VPN is required.

The tunnel daemon (cloudflared) runs as a lightweight service on your server, establishing an encrypted outbound connection to Cloudflare's edge network. CEOJuice's MCP server communicates through Cloudflare's infrastructure to reach your tunnel. At no point is your SQL Server directly addressable from the internet.

Encryption

All data in transit is encrypted with TLS 1.3. Cloudflare terminates TLS at their edge and re-encrypts to CEOJuice infrastructure. Cloudflare is acknowledged as a trusted intermediary in this architecture, consistent with their use by millions of enterprises globally.

Per-Client Isolation

Each dealer has a dedicated tunnel with a unique service token. Tunnel connections are not shared between dealers. There is no network path from one dealer's tunnel to another dealer's SQL Server.

Service Token Management

- Each dealer receives a unique Cloudflare service token during onboarding
- Tokens are rotated on a 90-day schedule
- Tokens can be revoked immediately by CEOJuice or by the dealer requesting deactivation
- A revoked token immediately disables the tunnel connection

Defense in Depth

The tunnel provides encrypted transport only. It does not grant SQL access. Even if the tunnel were compromised, an attacker would still need:

1. Valid SQL credentials (stored on the dealer's server, not transmitted through the tunnel)
2. To pass through the application-level query validator

3. To be limited to the permission scope set by the dealer's DBA

No single point of compromise grants unrestricted access to dealer data.

5. Tenant Isolation

Physical Isolation at the Data Source

Each dealer's e-automate database is a physically separate SQL Server on the dealer's own hardware, connected via a dedicated Cloudflare tunnel. There is no shared database between dealers. In a worst-case scenario where the CEOJuice MCP server is fully compromised, an attacker on Dealer A's tunnel cannot reach Dealer B's SQL Server. The isolation is architectural, not policy-based.

Memory Layer Isolation

The memory layer (which stores learned operational patterns) uses tenant-scoped identifiers at every layer. Each dealer's memory is accessible only through their tenant-authenticated API key. No MCP API call can return another dealer's memory data.

Planned Enhancements

As the platform scales, CEOJuice will implement additional database-enforced isolation in the memory layer, including PostgreSQL row-level security policies and dedicated cache namespaces. These are operational improvements for defense-in-depth. The current model already provides physical isolation at the data source and application-enforced isolation at the memory layer.

Verification

Tenant isolation is verified by automated tests that run on every deployment. These tests confirm that a request authenticated as Dealer A cannot access Dealer B's memory, telemetry, or tunnel.

6. Authentication & Access Control

Dealer Side

COMPONENT	AUTHENTICATION	DEALER CONTROL
SQL Server	Dedicated account, permissions set by dealer's DBA	Dealer's DBA controls permissions and can revoke at any time
Cloudflare Tunnel	Per-dealer service token, 90-day rotation	Dealer can request immediate revocation

CEOJuice Side

COMPONENT	AUTHENTICATION	SCOPE
MCP API	API key per tenant	Validated on every request. No shared keys between dealers.
Infrastructure	Environment-injected secrets	Production credentials managed via secrets manager. No hardcoded values.

No Interactive Access

The MCP platform cannot open an interactive remote session to your server. The Cloudflare tunnel supports only structured API calls (tool invocations that execute specific queries). There is no shell, no RDP, no remote desktop, and no file system access. This is more restrictive than the current CEO Juice Core model, which uses LogMeIn for interactive remote sessions.

7. AI / LLM Security

Current Provider

The MCP platform currently uses **Anthropic Claude** via their enterprise API for intelligent response generation.

- **Data retention:** Anthropic's API does not retain inputs or outputs beyond the request lifecycle. Your data is not used for model training. This is governed by Anthropic's API Data Usage Policy.
- **Certifications:** Anthropic holds SOC 2 Type II and ISO 27001:2022 certifications.
- **Processing location:** API requests are processed in Anthropic's secure infrastructure. See Anthropic's Trust Center for details.

Provider Flexibility

The platform architecture is provider-agnostic. CEOJuice can change LLM providers without any dealer-side changes, tunnel modifications, or data migration. CEOJuice selects providers based on enterprise security posture, zero-retention API policies, and applicable compliance certifications. Open-source models without equivalent security certifications are not used.

Dealers will be notified in advance of any LLM provider change. If a dealer requires a specific provider for compliance reasons, the architecture supports per-tenant provider configuration.

What the LLM Sees

During the processing window, the LLM receives SQL query results (which may include financial data, customer names, and operational details) in order to generate an intelligent response. This data is not persisted by CEOJuice and is subject to the LLM provider's zero-retention policy. After the response is generated, the data is not intentionally persisted outside the dealer's own SQL Server.

What the LLM Does Not See

- Database credentials or connection strings
- Other dealers' data
- CEOJuice system internals or infrastructure details
- The Cloudflare tunnel configuration

8. Memory Layer

Purpose

The memory layer enables the platform to learn each dealer's operational patterns over time. Instead of treating every question as a first-time interaction, the system builds context: which processes the dealer monitors most, which recommendations they act on, and which patterns tend to recur. This is the core value proposition of the platform and the primary reason it improves with use.

What Is Stored

CATEGORY	EXAMPLES	CONTAINS BUSINESS DATA?
Schema facts	Table names, column relationships, data types from your e-automate configuration	No. Structural metadata only.
Operational patterns	"This dealer prioritizes AR aging reviews weekly." "Branch 3 performance is reviewed quarterly."	No. Behavioral metadata.
Causal chains	"Billing divergence detected → cause: sync lag → resolution: trigger resync"	May contain incidental references (see below).
Session context	Task history, tool call sequences, abbreviated findings	May contain incidental references (see below).

Dealer-Specific References in Memory

Free-text fields in the memory layer (anomaly descriptions, causal chain symptoms, session findings) may contain dealer-specific references such as customer names, account identifiers, or branch names. For example, a detected pattern might reference "billing divergence for Customer ABC at Branch 5."

These references exist as part of the learned patterns that make the system useful. They are:

- **Tenant-isolated:** accessible only through your authenticated MCP session

- **Not visible to other dealers** or to CEOJuice employees through normal operations (see employee access below)
- **Exportable and deletable on request**

What Is NOT Stored

- Raw query result sets (financial reports, customer lists, invoice details)
- Bulk financial data (revenue figures, account balances, payment amounts)
- Complete customer records
- Invoice line items or transaction details

Employee Access

Memory layer content is accessible only through the tenant-authenticated MCP API. CEOJuice does not maintain an internal admin panel or query tool that exposes memory content.

In rare debugging scenarios where direct access to memory data is necessary to resolve a dealer-reported issue, a senior engineer may enable temporary access with the following controls:

- Explicit dealer authorization is required before access is granted
- Access is logged with the engineer's identity, timestamp, and reason
- Temporary access is revoked and logs are revoked promptly after the session concludes

Embedding Model

The memory layer uses a text embedding model to enable semantic search (finding related patterns by meaning, not just keywords). The embedding model processes schema metadata and operational summaries. Embeddings are one-way mathematical vector representations that cannot be reverse-engineered into the original text. They are stored in the tenant-isolated vector database.

Fleet-Wide Aggregation

CEOJuice uses anonymized, aggregated metadata across the dealer fleet for product improvement. Examples: "which tools are most used," "which error patterns are most common across the fleet," "which process categories generate the most questions."

- Aggregated metrics are only included when representing **3 or more distinct tenants**

- No individual dealer's patterns, memory content, or behavioral data is exposed to other dealers or externally
- Aggregation is performed on telemetry metadata (tool IDs, timestamps, error codes), not on business data or memory content

9. Data Retention & Deletion

DATA TYPE	RETENTION	CONTAINS BUSINESS DATA?
Query results	Not retained. Processed in-memory, not persisted to any application-level storage.	No
Telemetry metadata	Retained for the life of the service (operational monitoring)	No. Tool IDs, timestamps, error codes only.
Memory layer	Retained for the life of the service (this is the value — it improves over time)	Incidental references possible (see Section 8)
Embeddings	Retained for the life of the service in tenant-isolated vector database	No. One-way vectors, not reversible.

Deletion on Request

- **Active data:** purged within a commercially reasonable period of request, typically 30 days
- **Backups:** purged on the next backup rotation cycle following active data deletion
- **Confirmation:** dealer receives written confirmation of deletion completion

Offboarding

If a dealer terminates the MCP service, all tenant data is deleted: memory layer, telemetry, embeddings, session history. Tunnel credentials are revoked immediately. Deletion follows the same 30-day schedule as on-demand requests.

10. Incident Response & Availability

Outage Impact

The MCP platform is an additive intelligence layer. If it experiences an outage:

- Your e-automate system continues operating normally
- CEO Juice Core continues processing alerts and notifications
- All existing email alerts, reports, and automated processes are unaffected
- No dealer data is at risk during an outage (raw business data is not stored centrally)

Breach Notification

If CEOJuice confirms a security incident involving dealer data (including memory layer content), affected dealers will be notified promptly. Notification will include: nature of the incident, data potentially affected, remediation steps taken, and contact information for follow-up. Specific notification timelines are governed by the applicable service agreement.

Audit Trail

All tool calls are logged with dealer ID, tool ID, timestamp, and success or error status. Logs contain operational metadata only — not raw SQL text or query results. Dealers can request audit logs of all activity on their account through their CEOJuice account manager.

Availability

Uptime commitments are governed by the commercial service agreement and are outside the scope of this security document.

11. Operational Security

CEOJuice Team Access

- Production infrastructure access is limited to senior engineering staff
- CEOJuice operational practices prohibit employees from accessing raw query results. Results are not persisted to any log, database, or storage accessible to employees.
- Memory layer content is accessible only through the tenant-authenticated MCP API. There is no internal admin panel or bulk export tool for employee use.
- Break-glass debugging access requires explicit dealer authorization, is logged, and is revoked promptly after the session concludes (see Section 8).

Infrastructure

- Hosted on AWS with standard security practices: VPC isolation, security groups, encryption at rest (AES-256)
- Cloudflare for tunnel management and edge security
- Deployment pipeline includes automated tenant isolation verification on every release

Credential Management

Production credentials are injected via environment variables from a secrets manager. No credentials are hardcoded in application source code or configuration files.

Appendix A: Technical Specifications

SPECIFICATION	DETAIL
Transit encryption	TLS 1.3 via Cloudflare Tunnel
At-rest encryption	AES-256 for memory layer storage
SQL access scope (launch)	SELECT only. No EXECUTE, CREATE, ALTER, DROP, INSERT, UPDATE, DELETE. Future scope changes require dealer DBA action.
Query validation	Word-boundary regex blocking DML keywords, injection patterns (;, --, xp_, sp_), and statement chaining
Service tokens	Per-dealer Cloudflare service tokens, 90-day rotation. Revocable on demand.
Network requirements	Outbound TCP 443 only from dealer server. No inbound ports.
Tunnel daemon	cloudflared — lightweight service, minimal resource footprint (~64 MB RAM, negligible CPU), auto-updating
Parameterized queries	Pre-built tools use ? placeholders with typed parameters. No string concatenation in SQL construction.

Appendix B: Compliance & Certifications

LLM Provider (Anthropic)

- SOC 2 Type II
- ISO 27001:2022
- Zero data retention for API customers
- Details: *trust.anthropic.com*

Cloudflare

- SOC 2 Type II
- ISO 27001
- FedRAMP Moderate (Li and Connect)
- Details: *cloudflare.com/trust-hub*

CEOJuice

The certifications listed above belong to CEOJuice's infrastructure and AI partners, not to CEOJuice directly. CEOJuice's own security practices are described in this document. Independent certification is on the roadmap and timeline will be communicated as it is established.

Appendix C: FAQ for IT Teams

Can CEOJuice see our financial data?
Raw financial data is processed in-memory and not persisted to any application-level storage. The memory layer may contain dealer-specific references within pattern descriptions (e.g., a customer name in an anomaly finding) but does not store bulk financial records. Memory data is tenant-isolated and deletable on request.

What firewall changes are required?
None. The Cloudflare tunnel uses outbound TCP 443 only. No inbound ports are opened.

Who is the AI provider?
Currently Anthropic Claude, with a zero-retention API policy and SOC 2 Type II certification. The architecture is provider-agnostic and CEOJuice will notify dealers before any provider change.

What happens if we stop using the service?
All data is deleted: memory layer, telemetry, embeddings, session history. Tunnel credentials are revoked immediately.

Can other dealers see our data?
No. Enforced at the network level (separate tunnels to separate SQL Servers), and at the application level (tenant-scoped memory with authenticated API access). There is no shared data path between dealers.

How is this different from CEO Juice Core?
Same trust model, more structured. Read-only at launch. No interactive remote access. Multi-layer query validation. Zero raw data persistence on CEOJuice infrastructure. Any future write capabilities require your explicit approval.

Can we audit what queries were run?
Yes. Request audit logs through your CEOJuice account manager. Logs include tool ID, timestamp, and success/error status for every tool call. Logs contain operational metadata — not raw SQL text or query results.

What if we need a specific AI provider for compliance?
The architecture supports per-tenant provider configuration. Discuss requirements with your account manager.

Does CEOJuice share our data with other dealers?

No. CEOJuice performs fleet-wide analysis only on anonymized telemetry metadata (tool usage frequency, error patterns) and only when representing 3 or more dealers. No individual dealer's data, memory content, or behavioral patterns are shared.

> This document describes CEOJuice's current security practices and architecture as of the publication date. It is provided for informational purposes and does not constitute a warranty, guarantee, or contractual commitment. Security practices may evolve as the platform develops. Terms governing the MCP service are set forth in the applicable service agreement. The FAQ section is a summary; the detailed sections of this document govern in the event of any discrepancy.
