PARTNER AND MARKETPLACE BRIEF · MAPPED TO NIST SP 800-207

Syrebrum + Failstop: Zero Trust for AI agents

A command center for the computers and AI you already have, with policy enforced outside the model and a person in the loop.

The problem

An AI agent that can act is useful — and, without limits, a liability. Rules that live only as a prompt can be misunderstood or talked around. If the model is also the policy, the policy is not trustworthy.

The solution

Syrebrum is the command center. Failstop is the deterministic policy layer in front of anything that can act. Policy is enforced in software the model cannot change. AI seats may read, draft, and propose. They cannot approve a payment, clear a stop, or rewrite the rules. A person stays in the loop.

What it does today

- One command center for Windows, Ubuntu, Debian, and TrueNAS machines, and for the AI tools you already pay for.
- Bring-your-own keys for Claude, OpenAI, Gemini, Grok, Llama (through OpenRouter or Groq), and local models through Ollama.
- Payments, contracts, outreach, and security-setting changes always wait for the owner. A pause switch stops outbound work. Automatic actions are recorded. A read-only security checkup is available.
- Failstop checks proposed actions against fixed rules and writes a hash-chained audit log. Only the owner can approve a change or clear a stop. No AI can approve.

NIST SP 800-207 mapping, in brief

Failstop and Syrebrum's approval gates act as the Policy Engine, Policy Administrator, and Policy Enforcement Point, separate from the language model. Access is granted per action, re-checked at approval time, and recorded. This aligns with the tenets and components of NIST SP 800-207. It is not a claim of NIST certification or formal compliance.

Integrations

Connect the models and accounts you already use. Business connectors for Google, Microsoft 365, Square, and social networks are in beta and ask for the least access they need. Syrebrum is not a Google, Amazon, Microsoft, or xAI product, and this brief does not claim an official partnership with those companies.

Contact. CCD Enterprise & Development LLC · info@syrebrum.com · (337) 333-4091 · syrebrum.com

Syrebrum is beta software for your own computers and accounts; it is not a safety-rated system. Provider names are trademarks of their respective owners. Syrebrum is not affiliated with or endorsed by those companies.