

SYNQLY ARQ FOR ENTERPRISE

Synqly Arq: The AI Security Engineer Multiplier

Connect, Govern, Analyze, and Act

PROBLEM

Security leaders are accountable for outcomes across a stack that was never designed to operate as one. A typical enterprise SOC runs over 86 disconnected security tools from SIEMs, EDRs, identity providers, CSPMs, vulnerability scanners, to ticketing systems, and each comes with its own API, schema, auth model, and rate limits.

Integrating the security tools point-to-point requires building individual integrations, consuming 60% of security engineering capacity from development through support. Generic IPaaS tools handle plumbing but lack native support for security telemetry and aren't architected for security and IT use cases.

SOLUTION

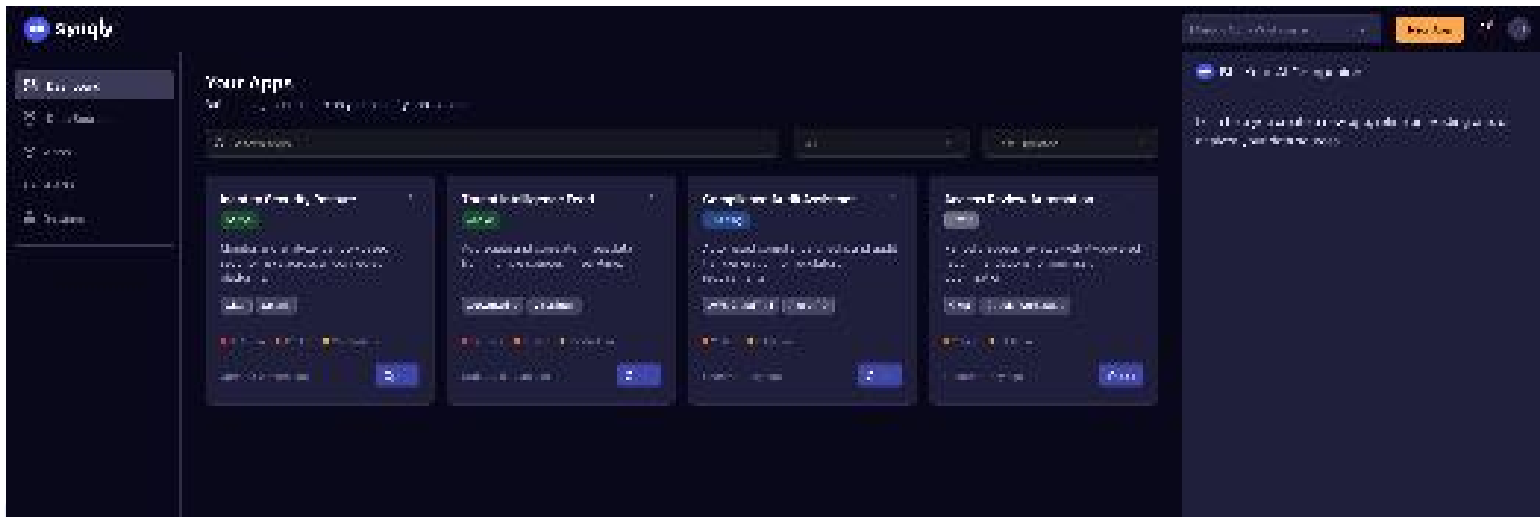
Synqly Arq for enterprise connects your IT and security products, creating a unified, bi-directional data plane. Investigations and everyday tasks can be initiated in plain language, while actions remain governed and auditable in the downstream systems. Your security team gains a governed way to ask questions of their existing tools, get consistent answers, share data across products, and turn outcomes into action.

Synqly is a production-deployed, cloud-native platform that unifies complex security ecosystems and data, and exposes it to AI agents through three tightly integrated layers:

- **AI Agent Orchestration:** Synqly's Agent Service runs a structured LLM execution loop with assembled prompts, multi-provider model routing, and Synqly MCP. Specialized subagents access data, evaluate alerts, and Arq response actions over the same OCSF surface with ease.
- **Unified API and Data Normalization:** Synqly connects to 100+ security vendors across 11 connector categories, transforming and normalizing raw vendor events into the Open Cybersecurity Schema Framework (OCSF) at speed.
- **Visualization and Reporting:** Unified API layer enabling visualization and reporting around common activities and ongoing jobs

With Synqly Arq, enterprise security analysts can type “Find all S3 buckets out of SOC2 compliance based on the last 30 days of CloudTrail and GuardDuty data.” Within seconds, Synqly streams a structured, normalized answer drawn from real telemetry with no manual coding, no integration reconfiguration, and no vendor-specific knowledge required.

Beyond rapid AI-driven threat investigations, Synqly Arq provides the foundation required for ongoing security operations. It continuously monitors security events, manages integration configurations, and ensures reliable data refreshes. Most importantly, it enforces strict operational governance by requiring human-in-the-loop approvals before any high-risk response actions are executed.



KEY CAPABILITIES

- Custom AI agents that help integrate with security tools and orchestrate common security tasks and analyses
- Customizable OCSF-based schema decouples AI reasoning from vendor-specific field naming, eliminating the need for reintegration when vendors change schemas
- Comprehensive RBAC controls govern the entire stack, ensuring full authority over data access and data sovereignty
- Deterministic API and database transactions drive ongoing security operations, ensuring predictable, repeatable, and reliable results
- Bridge Service extends connectivity into air-gapped and on-premises environments

With Synqly Arq, security teams maintain a single integration pattern, standard schema, and a mapping model that evolves without bespoke code. Synqly converts the integration debt that consumes most of security engineering capacity into a normalized, AI-addressable data surface, collapsing weeks of pipeline work into a single natural-language query and providing security teams with a unified substrate for detection, investigation, and automated response.

ABOUT

Synqly is The Connected Platform for Security, IT, and AI. Our unified API turns integrations into technical advantages, cutting development effort by up to 90%. We enable providers to deliver the connections their customers demand, and continue to set the standard for scalable, secure, and efficient integrations across the industry.