synqly

Power Your Cyber Ecosystem with
Synqly's AI-Enabled Integration Platform

SYNQLY MCP

Synqly MCP: AI Meets Security Integrations

Synqly MCP and a few lines of code deliver native integrations with the largest integration ecosystem in cybersecurity and IT operations

PROBLEM

Cybersecurity providers are under growing pressure to deliver seamless, scalable integrations across a diverse ecosystem of tools and platforms, and the rise of AI assistants and agentic systems has turbocharged the need for connections across products. Each vendor's AI feature operates in isolation, unable to communicate or collaborate across systems. Meanwhile, integration development remains slow, code-heavy, and brittle, often requiring custom scripting, UI workarounds, or months of engineering effort that doesn't scale.

SOLUTION

Synqly Model Context Protocol (MCP) is the first MCP Server purpose-built to support AI agents in security and IT operations, delivering a structured, secure interface that allows agentic systems to stream data, enrich context, and take real-time action across the largest cybersecurity integration ecosystem.

Synqly's unified API enables vendors to integrate with entire product categories in days. Synqly MCP takes it further, offering access to the largest ecosystem of security and IT operations solutions, with integrations possible in just hours. Integration setup, data access, and automation are now accessible to AI assistants through a single protocol, accelerating time-to-value and enabling collaboration between previously siloed systems. With Synqly MCP, agentic AI can reason across integrations, act in real time, and adapt to new signals on demand, without custom code.

Synqly MCP sits between AI systems and the integration ecosystem, acting as a universal access layer. With support for bi-directional streaming, agent-driven queries, and dynamic control, Synqly MCP unlocks proactive automation, autonomous response, and continuous optimization across the tech stack. Integrated platforms become more than data sources; they become intelligent surfaces for action, discovery, and control.

USE CASES

Security vendor's agentic AI solutions have exponentially more value as they have access to more data. Traditional engineering practices of one-off integration building is too slow and expensive and results in missed potential of the AI investment.

Synqly MCP instantly connects AI agents the largest ecosystem of security and IT operations solutions. The unified interface across integrations provides AI agents with the data they need in an easy to analyze format.

- Faster time to market
- Expanded AI capability and results
- Reduced engineering overhead; engineers can focus on value core to the business

Managed Security Service Providers (MSSPs) must deploy, manage, and maintain dozens or even hundreds of unique integrations across multiple customer environments. Manual setup is time-consuming, error-prone, and doesn't scale.

With Synqly MCP, an AI agent can establish, configure, and validate integrations for each customer, without custom scripts or UI interaction.

- Consistent, auditable integration rollout
- Scalable onboarding of new customers with minimal overhead and customer impact
- 90% reduction in time spent per integration

SaaS security vendors supporting integrations for customer tenants often struggle with fragmented setup and maintenance workflows across environments.

Synqly MCP enables vendor-hosted agents to manage customer integrations: listing, updating, and monitoring them across tenants with scoped access.

- Drastic reduction in support tickets related to integration setup and maintenance
- Centralized observability and management of all customer integrations

Enterprises operate sprawling environments with dozens of security and IT tools deployed across business units, subsidiaries, and regional teams that rarely interoperate. Data is siloed across division and security operations struggle to gain full visibility and make the most of expensive security solutions.

Synqly MCP introduces a structured integration layer that allows organizations to connect previously isolated tools through a common protocol. Whether via in-house agents or vendor-native copilots, security teams gain unified access to telemetry, alerts, posture data, and configuration settings.

- Consolidated visibility across complete
- ecosystems
- Improved signal correlation, incident response, and reporting accuracy
- Greater return on security investments through centralized access and automation

SYNQLY ADAPTIVE DATA MAPPING DELIVERS:

- **Protocol Built for AI Agents:** MCP is the first integration layer designed with AI agents as the core user, supporting real-time queries, data streaming, and control pathways natively.
- **Seamless Ecosystem Access:** Direct connectivity to Synqly's unified API across EDR, SIEM, ticketing, cloud security, identity, and more.
- **AI-Native Enrichment and Actions:** Agents can enrich data with system-specific context and trigger workflows directly, streamlining alert triage, asset discovery, policy enforcement, and more.
- **No Custom Code or UI Hacking Required:** Removes dependency on UI automation, brittle scripts, or one-off dev work by exposing standardized capabilities through the MCP layer.
- **Unified Control at Runtime:** Your agentic AI can manage integration state, configuration, and mappings on the fly, reducing maintenance burdens and operational drag.

ABOUT

Synqly is the first integration platform purpose-built for security, IT Ops, and Managed Service vendors. Our unified API enables rapid, seamless integrations, without draining engineering resources, reducing development costs and complexity by up to 90%. Synqly sets the new standard for scalable, efficient security integrations.

synqly