Synapse

Platform Operations Suite

SAP Commerce Cloud Edition

"AI-powered monitoring, diagnosis and autonomous response for SAP Commerce Cloud — secure, private, and always in your control."

PRODUCT SNAPSHOT

Product	Synapse — Platform Operations Suite
Edition	SAP Commerce Cloud
Vendor	Jarvis Business Solutions (jarvisbusiness.io)
Deployment	SaaS — cloud-hosted, credentials encrypted at rest
Pre-requisites	SAP Commerce Cloud (Hybris) · Dynatrace APM · Azure Blob log storage
Onboarding	Under 30 minutes from sign-up to first live diagnostic
AMS option	Jarvis AMS support available at Essential, Standard, and Premium bands

01 WHAT IS SYNAPSE

The operating system for your SAP Commerce Cloud platform

Enterprise SAP Commerce Cloud environments are complex by nature. Dozens of interdependent services, a continuous stream of events across ImpEx imports, catalog updates, order pipelines, search indices, and cache layers — and the operational tooling to manage it all has not kept pace. Engineers spend 30–45 minutes triaging every incident manually. ImpEx errors reach production. Cache degradation goes undetected until customers notice. Deploy confidence depends on someone remembering to check the right dashboard at the right time.

Synapse is Jarvis's answer to that gap. It is a Platform Operations Suite purpose-built for SAP Commerce Cloud — running always-on AI agents that continuously monitor your environment, developer tools that surface intelligence on demand, and autonomous playbooks that respond to incidents without human intervention. It understands the specifics of your platform: ImpEx files, Hybris cronjobs, Solr indices, OMS order flows, HAProxy cache layers, and SAP-provisioned Azure log containers. No generic APM tool does.

Synapse is structured as a four-tier progressive stack. Every customer starts at Foundation and unlocks additional intelligence capability as they progress through Monitor, Predict, and Automate. You can enter at any tier and scale at your own pace.

	01 Foundation *Validate & Baseline* Weeks 1–2	**02 Monitor** *Live Agent Monitoring* Weeks 3–5	**03 Predict** *Predictive Intelligence* Weeks 6–8
04 Automate *Autonomous Response* Weeks 9–12	Connect 5 data sources. Validate credentials. Establish a 30-day KPI baseline so Synapse learns what your environment's normal looks like before raising a single alert.		

Monitor	**Eight always-on AI agents run continuously across Detection & Diagnosis and Commerce Intelligence. Real-time alerts calibrated against your 30-day learned baseline — targeting under 5% false positive rate.**
Predict	Four ML models trained on your baseline: LSTM traffic forecasting, Isolation Forest anomaly detection, capacity planning signals, and deployment risk scoring. Transforms your support posture from reactive to anticipatory.
Automate	Three incident playbooks — rollback decisions, cache recovery, P2 triage — run in shadow mode for 30 days before full automation is enabled. Your team approves the first 10 executions before the system acts autonomously.

02 HOW IT WORKS

Five connectors. Eight agents. Continuous intelligence.

Synapse connects to your SAP Commerce Cloud environment through five native connectors. Each connector feeds a different class of operational intelligence into the Synapse pipeline. Together they give Synapse complete visibility across infrastructure, commerce logic, search, logs, and storage — the five layers where SAP Commerce Cloud issues originate.

The five data connectors

Connector	What it provides
Dynatrace APM	Performance metrics, problem events, entity topology, host CPU and memory, application response times and error rates. Foundation of real-time health monitoring and the primary input for Log Intelligence root cause analysis.
OCC REST API	SAP Commerce Cloud's native headless interface. Synapse uses it to query product catalog quality, order pipeline status, active promotion integrity, and checkout functional health — the commerce logic layer that infrastructure tools cannot see.
Solr	Search index freshness, query error rates, core document count trends, and Solr memory health. Detects the invisible degradation — stale indices, query failures — that causes conversion loss without triggering any infrastructure alert.
OpenSearch	Application log streams in real time. Stack trace fingerprinting and deduplication, log volume trending, and new error pattern detection. Powers Log Intelligence root cause analysis and the SupportAgent triage tool.
Azure Blob	SAP-provisioned log container including system logs, deployment logs, and support bundles. AI-powered clustering of ERROR and WARN patterns. Used for post-incident forensics, deployment validation, and on-demand SupportAgent queries.

Eight always-on monitoring agents

Once the 30-day baseline period is complete, eight agents run continuously — comparing live signals against your learned environment profile and alerting only when deviation is statistically significant.

Tier 2 — Detection & Diagnosis

Agent	Function

Real-time Health Monitor	KPI and SLA tracking against learned baselines — response times, error rates, host CPU and memory. Alerts only on statistically significant deviation. Targets under 5% false positive rate.
Log Intelligence	Correlates Dynatrace problem events with metric anomalies to produce root cause hypothesis and fix steps. Reduces mean triage time from 30–45 minutes to under 15 minutes.
Error Pattern Classifier	Fingerprints recurring exceptions by stack trace, tracks frequency and velocity, and surfaces one prioritised alert per pattern rather than flooding the queue with duplicates.
Dependency Failure Tracker	Monitors all outbound API calls to third-party services — payment gateways, tax engines, logistics APIs. Detects latency spikes and circuit breaker events before they cascade into order failures.

Tier 4 — Commerce Intelligence

Agent	Function
Catalog Integrity	Scans product data quality continuously via OCC — detects zero prices, missing descriptions, broken images, and bad category assignments. Catches problems introduced by ImpEx imports and ERP feeds before they reach the storefront.
Order Flow Watchdog	Monitors the order state machine in real time. Detects PAYMENT_PENDING and ORDER_PROCESSING timeouts, order volume anomalies (a proxy for checkout failures), and B2B approval workflow blockages.
Search & Solr Health	End-to-end search pipeline monitoring — from Solr index freshness through to OCC functional search checks. Detects index staleness and query failures before customers experience zero search results.
Cache Optimisation	Tracks HAProxy and Hybris cache hit rates against baseline. Alerts on drops that are leading indicators of performance degradation, before origin server load reaches the point of customer impact.

03 DEVELOPER TOOLKIT

Seven on-demand tools — always available in the toolbar

In addition to the always-on agents, Synapse provides seven developer tools that engineers run on demand without leaving the platform. These tools are designed specifically for the SAP Commerce Cloud operational workflow — not generic log search or APM queries, but purpose-built analysis that understands ImpEx, Hybris, Solr, and OCC natively.

Tool	What it does
Log Intelligence	Full Dynatrace telemetry analysis — correlates problems, metrics and entity topology to produce root cause and actionable fix steps for any incident. Run on demand for deeper investigation beyond the agent alerts.
ImpEx Validator	18 static rules covering SAP Commerce Cloud ImpEx syntax, data type constraints, and catalog structure — plus Claude AI semantic review. Returns a go/no-go recommendation before any import is executed in production. Prevents the class of data corruption that most commonly causes catalog and order failures.
Deploy Diff	Pre/post snapshot comparison for every deployment. Detects error rate spikes, response time regressions, and new exception types introduced by a release. Produces a STABLE or ROLLBACK verdict with supporting evidence.
Code Review	12 static pattern rules covering SAP Commerce Cloud anti-patterns — Jalo layer usage, Hibernate bypass, System.exit calls, and empty catch blocks — plus Claude AI review for thread safety and performance issues. Runs on every commit.
Data Integrity	OCC deep validation — scans prices, catalog quality, order data, active promotions, and inventory levels for inconsistencies that monitoring agents may not surface. Useful pre-launch and post-import.
Git Integration	Read-only scan of Bitbucket, GitHub, GitLab, and Azure DevOps. Reviews pull requests, scans repositories for anti-patterns, and validates ImpEx files inline in the development workflow — without requiring engineers to leave their existing tools.
Log Ingestion (SupportAgent)	Reads the SAP-provisioned Azure Blob log container, clusters ERROR and WARN patterns using AI, and provides triage with severity scoring and recommended resolution steps. Ask SupportAgent natural language questions about your logs.

Git Integration and Log Ingestion (SupportAgent) require the Growth or Enterprise subscription tier.

04 PRE-REQUISITES & COMPATIBILITY

What you need before you connect

Synapse is designed for rapid connection — most environments are live within 30 minutes of signing up. The pre-requisites below must be in place before onboarding begins. Jarvis will confirm each item during the initial scoping call.

Platform requirements

Requirement	Detail
SAP Commerce Cloud (Hybris)	Any supported version of SAP Commerce Cloud. Synapse has been validated against Hybris 6.x, 1905, 2005, 2105, 2205, and 2211. Earlier versions are supported but should be confirmed during scoping.
Dynatrace APM	An active Dynatrace environment monitoring your SAP Commerce Cloud deployment. Synapse connects via the Dynatrace API v2 using a read-only API token. A Dynatrace licence is required independently of Synapse — it is not included.
OCC REST API	OCC must be enabled and accessible. Synapse uses a read-only service account with access to catalog, order, and product endpoints. No write access is required or requested.
Azure Blob Storage	SAP Commerce Cloud on Azure provisions a Blob storage container for platform logs. Synapse requires read access to this container via a SAS token or storage account key with read-only permissions.
Snowflake or OpenSearch	At least one log analytics target must be available — either OpenSearch (for the application log connector) or access to log streams via Azure Blob. Both are supported; OpenSearch provides richer real-time querying capability.

Access requirements

Access item	What Jarvis needs
Dynatrace API token	Read-only API token with access to problems, metrics, entities, and topology. Generated by the customer in the Dynatrace console. Synapse stores it encrypted at rest.
OCC / SCAPI credentials	Service account username, password, and base URL for your OCC endpoint. Read-only access to catalog, products, orders, and promotions.
Solr connection details	Solr host, port, and core name(s). Read-only access. Network must allow Synapse to reach the Solr endpoint.

Azure Blob SAS token	A Shared Access Signature (SAS) token with read permissions on the SAP-provisioned log container. Generated by the customer with a defined expiry — Synapse will alert when the token is within 30 days of expiry.
Git provider token (optional)	Read-only personal access token or OAuth token for Bitbucket, GitHub, GitLab, or Azure DevOps. Required only if the Git Integration developer tool is activated.
Network / firewall	Synapse's SaaS infrastructure must be able to reach your Dynatrace API endpoint, OCC base URL, Solr host, and Azure Blob endpoint. No inbound ports are required. Outbound HTTPS (443) from Synapse to those endpoints must be permitted.

What Synapse does not require

Synapse is designed with a minimal-access principle. The following are explicitly not required:

- No SSH or remote shell access to any server
- No database credentials or direct database connections
- No write access to any SAP Commerce Cloud, Dynatrace, or Azure resource
- No agent installation on SAP Commerce Cloud servers
- No changes to SAP Commerce Cloud application code or configuration
- No VPN or network tunnel into the customer environment

All connectivity is outbound HTTPS from Synapse to your existing API endpoints. Credentials are encrypted at rest using Fernet symmetric encryption and decrypted only in memory during a live connector call.

05 OPTIONS & CONFIGURATION

Build the configuration that fits your environment

Synapse is not a one-size-fits-all subscription. You activate the connectors, agents, and playbooks your environment needs. Everything is available from day one — you choose what to switch on based on your operational priorities, team maturity, and platform configuration.

Data source options

Each connector is activated independently. You can start with one and add more at any time. Volume discounts apply automatically as you activate more sources.

Connector	Recommended if...
Dynatrace APM	You want real-time performance monitoring, root cause analysis, and the full agent suite. Dynatrace is required for the Real-time Health Monitor, Log Intelligence, Error Pattern Classifier, and Dependency Failure Tracker agents. Recommended for all engagements.
OCC REST API	You want commerce-specific intelligence — catalog quality, order flow monitoring, checkout health. Required for Catalog Integrity, Order Flow Watchdog, and Search & Solr Health agents. Recommended for all SAP Commerce Cloud deployments.
Solr	Your SAP Commerce Cloud uses Solr for search (standard for all Hybris deployments). Activating this connector enables the Search & Solr Health agent and provides direct index freshness monitoring independent of Dynatrace.
OpenSearch	You want real-time log stream analysis — new error pattern detection, log volume trending, and the deepest input for Log Intelligence. Recommended if you have OpenSearch deployed as your log analytics layer.
Azure Blob	You want access to SAP-provisioned platform logs for deep forensics, deployment validation, and on-demand SupportAgent AI queries. Required for the Log Ingestion developer tool. Recommended for all SAP Commerce Cloud on Azure deployments.

Monitoring agent options

Agents are grouped into two tiers. Detection & Diagnosis agents require Dynatrace to be connected. Commerce Intelligence agents require OCC REST API. Agents can be activated individually — you do not need to activate the full group.

Agent	Requires	Recommended if...
Real-time Health Monitor	Dynatrace	You want 24/7 baseline-calibrated alerting on infrastructure performance. Recommended for all deployments.
Log Intelligence	Dynatrace + OpenSearch or Azure Blob	You want automated root cause analysis reducing triage time. Recommended for all deployments.
Error Pattern Classifier	OpenSearch or Azure Blob	Your platform generates high log volumes and you want alert deduplication and pattern prioritisation.
Dependency Failure Tracker	Dynatrace	You integrate with external payment gateways, tax engines, or logistics APIs where failures impact checkout.
Catalog Integrity	OCC REST API	You run regular ImpEx imports or ERP data feeds where data quality issues could reach the storefront.

Order Flow Watchdog	OCC REST API	Revenue protection is a priority — you want early detection of stuck orders and payment pipeline failures.
Search & Solr Health	OCC REST API + Solr	Search is business-critical and you want end-to-end monitoring from index freshness to functional search response.
Cache Optimisation	Dynatrace + OCC REST API	You want early warning of cache performance degradation before it manifests as a P1 incident.

Automated playbook options

Playbooks are available from the Automate tier onwards. All three run in shadow mode for a minimum of 30 days before autonomous execution is enabled. During shadow mode, the playbook produces verdicts and simulates actions for human review — giving your team full confidence before automation goes live.

Playbook	What it does
Rollback decisions	Monitors the 30-minute post-deployment window and produces an automated STABLE or ROLLBACK verdict based on error rate delta, response time regression, new exception patterns, and order flow continuity. When in full auto mode, a ROLLBACK verdict triggers the rollback pipeline immediately.
Cache recovery	Detects cache hit rate drops and executes a configurable warm-up sequence to restore performance. Distinguishes between planned (post-deploy) and unplanned drops. Escalates to P2 if warm-up fails to restore within the defined SLA.
P2 triage	Automates the first 15 minutes of P2 incident response — severity scoring, multi-source evidence assembly, root cause hypothesis, affected journey identification, historical pattern matching, and routed delivery of the briefing to the correct team. Escalates to P1 automatically if conditions worsen within 20 minutes.

06 SECURITY & PRIVACY

Your code and data stay yours

"We designed the system so the AI receives the minimum possible information — and retains none."

Principle	How it is enforced

Filtered before it leaves	Two automated filters run on every AI submission. PII scrubbing removes email addresses, IP addresses, and tokens. Credential detection blocks the entire call if API keys, database passwords, or private keys are detected in the content.
Code never stored by AI	Anthropic's API does not retain or train on API inputs. Customer code and log data is processed in-session and discarded. No AI model is trained on proprietary customer data. Ever.
Encrypted at rest, always	All platform credentials are stored using Fernet symmetric encryption. Decrypted in memory only during a live connector call. API responses always mask credential values with ***. Credentials are zeroed immediately on account termination.
Isolated per customer	Data, credentials, scan history, and AI workspace are completely isolated between customers. Tenant isolation is enforced at the database query level — not solely at the application tier. No cross-tenant data access is architecturally possible.
Minimum access principle	Synapse requests only read access to all connected systems. No write access is requested, used, or stored. The automated playbooks operate by triggering existing CI/CD pipelines — they do not directly mutate any system.

07 JARVIS AMS SERVICES

Human expertise, always behind the intelligence

Synapse gives your team AI-powered intelligence. Jarvis AMS gives you the human expertise to act on it. The two are designed to work together — Synapse surfaces and diagnoses, Jarvis resolves. For organisations without a large internal SAP Commerce Cloud operations team, or those who want to extend their team's capacity without hiring, Jarvis AMS is available as an optional managed service alongside any Synapse configuration.

What Jarvis AMS covers

Service area	What is included
Incident management	Jarvis engineers receive Synapse alerts already briefed — root cause hypothesis, affected services, and recommended fix steps pre-populated. This eliminates the 30–45 minute manual triage step. Engineers act, not investigate.
Platform releases	Structured production release management with Deploy Diff pre and post validation, rollback support, and release notes documentation. Quarterly release allocations with emergency release cover.
Configuration management	Ongoing Synapse configuration management — agent threshold tuning, connector health, new data source activation, and quarterly baseline recalibration as your environment evolves.
Code & ImpEx review	Jarvis SAP Commerce Cloud architects review code changes and ImpEx files before they reach production — using Synapse's Code Review and ImpEx Validator tools as the baseline and adding human judgement for business logic and edge cases.
Enhancement services	Development capability for platform enhancements, bug fixes, and configuration changes beyond break-fix support. Available as a quarterly day allocation or on-demand sprint engagements.
Advisory & roadmap	Senior SAP Commerce Cloud architects available for platform direction, upgrade planning, and technology decisions. Available at Standard and Premium AMS bands.

AMS support bands

Band	Coverage	Best for
Essential	Email support · monthly config review · threshold tuning on request · up to 4 change requests per month	Teams with strong internal SAP CC capability who want Synapse

		managed but incidents handled in-house.
Standard	Named engineer · bi-weekly review · proactive agent tuning · up to 10 change requests per month · P1 out-of-hours cover	Teams who want a named Jarvis partner managing day-to-day operations and handling P1 incidents around the clock.
Premium	Dedicated architect · weekly review · unlimited configuration changes · roadmap advisory · 24/7 P1 cover for all severities	Organisations running mission-critical SAP Commerce Cloud where platform operations are a business-critical function and full coverage is required.

The AMS fee is calculated as a percentage of your Synapse platform cost — it scales automatically when you add or remove services. No separate commercial conversation required when your configuration grows.

The combined advantage

When Synapse and Jarvis AMS operate together, the support model shifts from reactive break-fix to proactive intelligence-driven operations. The table below summarises what the combination delivers compared to either capability in isolation.

Challenge area	Synapse alone	AMS alone	Synapse + AMS
Incident triage	AI root cause in <15 min	Manual log reading, 30–45 min	Engineer receives AI briefing before they engage. Resolves in minutes.
Code risk	Every commit scanned automatically	Senior dev review on request	Synapse flags; Jarvis architect reviews edge cases and fixes before deploy.
ImpEx risk	18-rule validator + AI semantic review	Manual check or missed entirely	Validated by Synapse + signed off by Jarvis engineer before execution.
Deploy confidence	STABLE / ROLLBACK verdict from Deploy Diff	Testing-phase discovery only	Jarvis executes rollback with full Deploy Diff context already in hand.
Capacity planning	ML forecasting 4+ weeks ahead	Reactive to incidents	Jarvis PMO uses Synapse ML signals to plan capacity proactively.

08 GETTING STARTED

Live in under 30 minutes

Synapse is designed for rapid onboarding. The four steps below take most customers from sign-up to their first live findings in under 30 minutes. No agent installation. No code changes. No infrastructure deployment on your side.

Step	Detail
01 · Sign up & select connectors 5 minutes	Create your Synapse account and select which data sources to activate — Dynatrace, OCC REST API, Solr, OpenSearch, Azure Blob. You only activate what you need.
02 · Connect credentials 10 minutes	Paste your connector tokens — API keys, service account credentials, and SAS tokens as applicable. Synapse encrypts everything immediately. One-click test per connector confirms connectivity. No tokens are ever logged or displayed after initial entry.
03 · Run first diagnostic 30 seconds	Click Run Diagnostic. Synapse queries all connected sources simultaneously and returns a severity-ranked report with root cause analysis and recommended actions. Real findings from live commerce data — no setup beyond credential entry.
04 · Connect Git & configure alerts 15 minutes	Optionally connect your Git provider (Bitbucket, GitHub, GitLab, Azure DevOps) with a read-only token. Configure alert routing to Slack, webhook, or email. Set team notification preferences. Your team is live.

Following sign-up, Synapse enters the 30-day baseline calibration period. During this time, all eight monitoring agents are active and learning your environment's normal. Predict tier ML models activate at the end of week 6. Automate tier playbooks enter shadow mode at week 9 and can be enabled for full autonomous execution after the 30-day shadow review period.

What to expect in the first 30 days

Timeframe	What happens
Day 1	First diagnostic complete. Severity-ranked findings from live platform data. Monitoring agents active and collecting baseline data.
Week 1–2	Baseline calibration in progress. Early alerts may fire on anomalies that fall outside initial estimates — these are reviewed and threshold-tuned during onboarding. If AMS is active, your Jarvis engineer manages this.
Week 3–5	Baseline established. Agent alert quality reaches target. False positive rate should be under 5% for most environments. Full agent monitoring operational.

Week 6–8	Predict tier activates. ML models begin producing forecasts and deployment risk scores against the calibrated baseline. Capacity planning signals available.
Week 9–12	Automate tier enters shadow mode. Playbooks produce verdicts and simulate actions — reviewed by your team or Jarvis AMS. Full autonomous execution enabled after 30-day shadow review.

09 NEXT STEPS

Ready to connect your SAP Commerce Cloud environment?

Step	What to do
Discovery call	A 30-minute call with Jarvis to map your current SAP Commerce Cloud environment — which connectors apply, what agents are most relevant, whether AMS is the right add-on for your team. No obligation.
14-day PoC	Connect your environment and run your first diagnostic at no cost. Trial runs on the full feature set. No card required. First findings within 30 minutes of connecting.
Scoping & proposal	If AMS is of interest, Jarvis will produce a tailored proposal covering connector configuration, agent selection, AMS band recommendation, and onboarding timeline based on your specific environment.
Integrated kick-off	Synapse connectors and agents activated in parallel with Jarvis AMS team onboarding (if applicable). First full monitoring coverage live within Week 1.

Get in touch
hello@jarvisbusiness.io | www.jarvisbusiness.io
Jarvis Business Solutions · A CX¹ Agency · Digital Transformation · Data · AI · ERP