SAP API Policy

PUBLIC

Agenda

01 API Policy (15 mins)

02 Non-Published APIs (5 mins)

03 Endorsed Architectures (10 mins)

04 Integration Suite MCP Gateway Demo (15 mins)

05 Q+A (15 mins)

API Policy

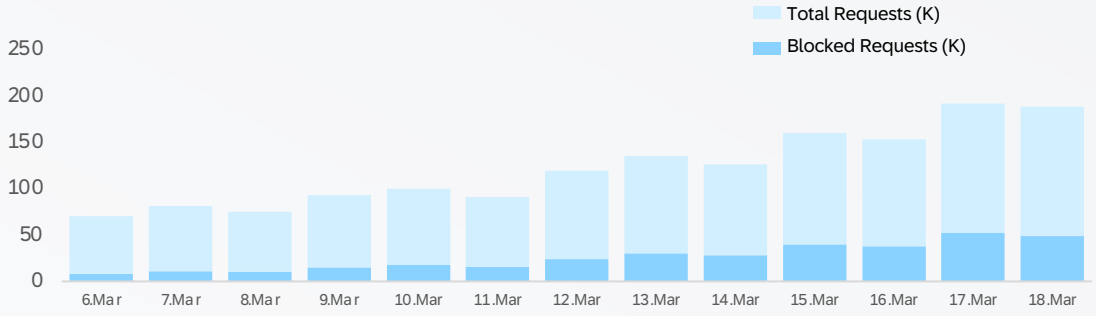
What is already happening

Forces Reshaping API Risk

- **The Scale Shift:** Automated AI traffic is growing several times faster than human activity and now accounts for a significant share of all requests creating unpredictable load spikes that request/response APIs were never built to absorb.
- **Ungoverned AI Risk:** Agentic AI traffic has surged dramatically over the past year, introducing "shadow agents" that can bypass traditional security perimeters and exploit protocol vulnerabilities

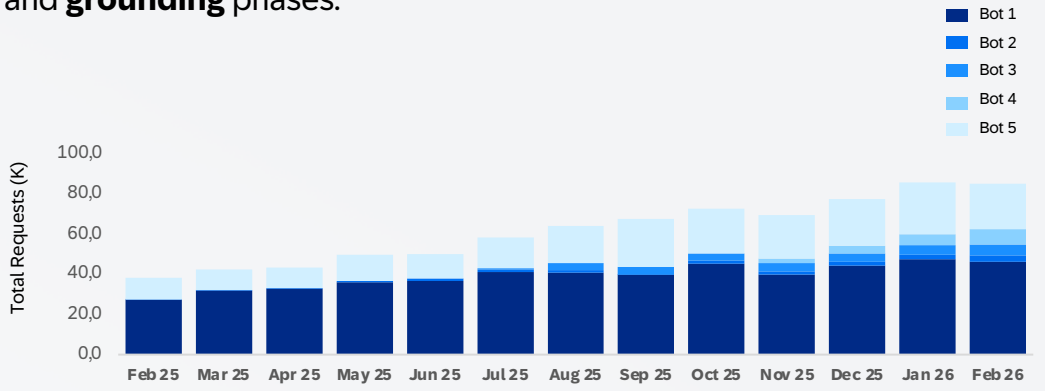
Structured Endpoints

AI agents scraping structured data are **driving traffic volumes** that **overwhelm** transactional API surfaces – the trend is accelerating.



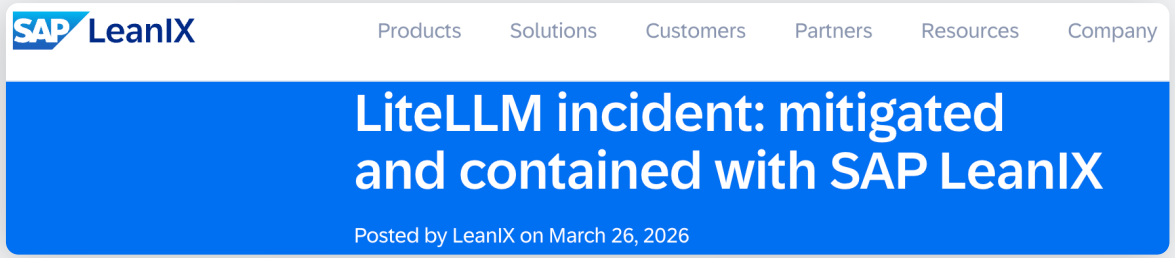
Unstructured Endpoints

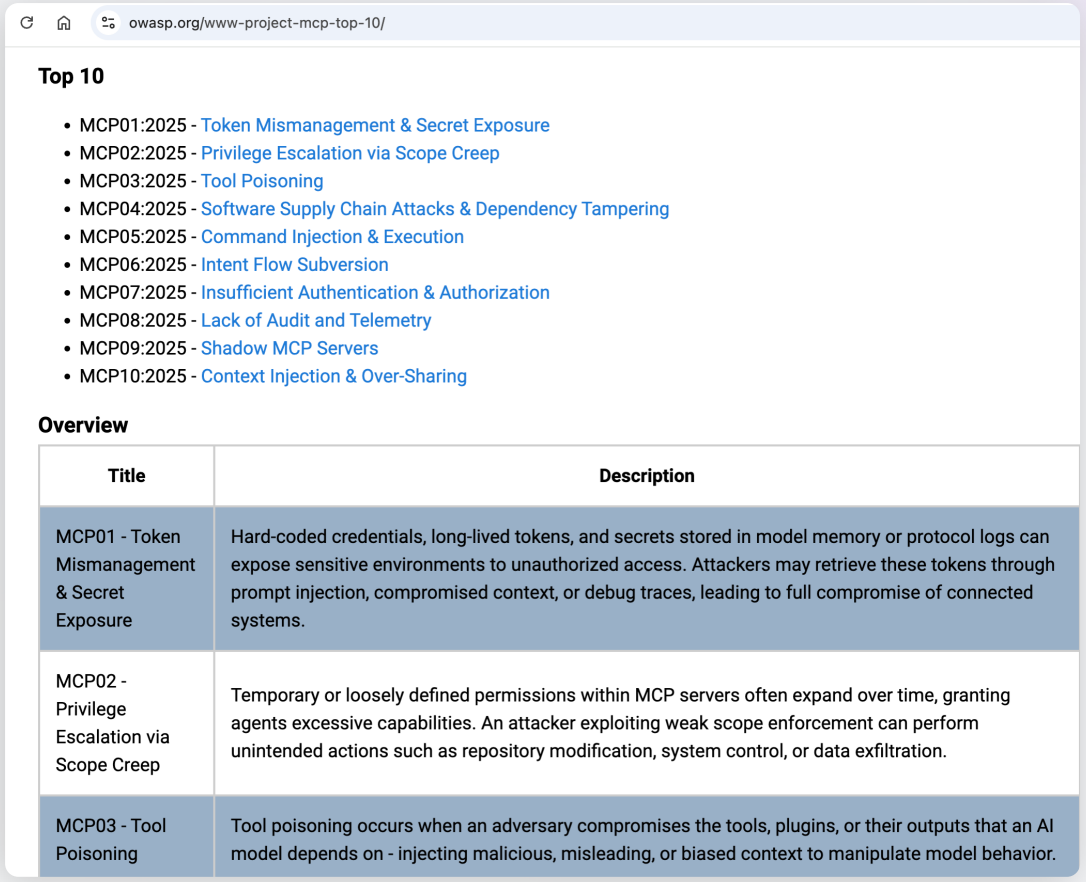
AI bots access data in **focused bursts** corresponding to their **training** and **grounding** phases.



Supply chain attacks targeting AI infrastructure

Why Toolchain Vulnerabilities are the Next Enterprise Security Blind Spot





Our approach is not to close the ecosystem

But to build the right infrastructure for an open one

1 Fair and secure service access for customers

API Policy

- **Published on April 27, 2026**
- **Outlines terms for** API availability, limits, usage, and monitoring
- **Enforces** usage of Published APIs and adherence to Documentation on SAP Help and product developer portals

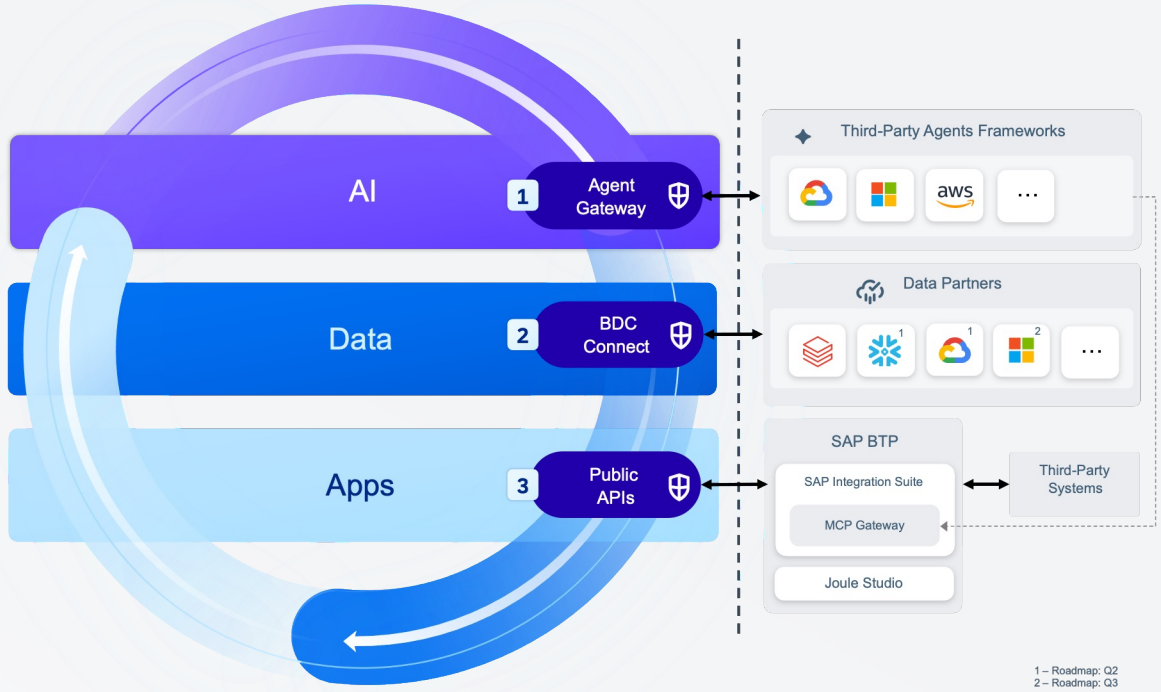
Industry-Standard API Protection & Fair Use

- **Unifying** rate limiting and workload management, where applicable, to maintain system stability and service health
- **Bot detection and AI safeguards** following industry best practices to protect system health from automated threats
- **Monitoring** to support policy compliance, maintain service health and support equitable performance for all customers.

2 Fit-for-purpose pathways for AI and Data

Endorsed AI and Data Access Patterns

- **Architectural guidance** for AI Agent integration through A2A (Agent Gateway), data sharing via zero copy primitives
- Refer to SAP Architecture Center and SAP AI Golden Path for details



How SAP APIs can be used

Clear guidance on availability, controls, and monitoring to ensure secure and reliable API consumption.

API Availability

Published APIs:

On the **SAP Business Accelerator Hub** or in **SAP product Documentation** are for their documented usage

Non-Published APIs:

- **What they are:** SAP-internal interfaces in SAP namespaces that are not documented as Published APIs.
- **Usage Status:** Use is at own risk as these are not supported.

API Controls

Specific Controls (Defined in Docs/ SAP Business Accelerator Hub):

- Technical rate limits and quotas – see Ariba, SuccessFactors, LeanIX for example
- Data ingress/egress quotas

General Controls

- Risking system performance, stability, or security.
- Large-scale data extraction or scraping or integration with autonomous AI agents, only via an endorsed SAP architecture.

Monitoring:

SAP monitors API usage to support compliance and platform stability.

How will we apply the policy?

- **Prioritizing dialogue:** The focus is on secure usage and open dialogue to ensure equitable access for all.
- **Automation Checks:** Will extend the Cloudification Repository with classifications for non-released and explicitly prohibited interfaces, enabling ATC checks to automatically flag non-compliant API usage.
- **Enabling our customers to use solutions that are designed for the new world of AI:** Providing fit-for-purpose solutions, reference architectures, and guidance to evolve towards an AI-native AI and Data architecture.

What are the benefits for our customers?

- **Stability for customer landscapes** and integrations, while creating opportunities to proactively improve performance and reliability.
- **A secure and reliable foundation** for building trustworthy AI solutions, accelerating your path from innovation to real-world business value.

* equitable access rate limits, throttling etc. are standard in the software industry.

Non-Published APIs

API Policy Does Not Impact Clean Core

Custom APIs that customers build in their own namespace for integration and extensibility remain unaffected

What the Policy Doesn't Prohibit

Customer-Built Custom APIs

Customer namespaces such as Z,Y -namespace interfaces, custom RFCs, OData services, CDS views, **remain permitted**. The policy restriction targets SAP's own internal APIs, not customer-developed code.

Existing Integrations & Extensions

Integrations using documented/published APIs for their intended purposes are **not to be impacted**. **Clean Core as a best practice** guidance remains.

Flexibility in Private Cloud Preserved

Customers **retain the ability to build and extend in their own namespace;** this freedom is not being revoked.

All permitted access is subject to the general API controls designed to protect platform stability and security, and must not be used to circumvent the policy, including **mass data egress** and **agentic access.**

How to Determine Allowed API Usage

Published APIs

Any API listed on SAP Business Accelerator Hub, SAP Help Portal, or dedicated product portals (e.g. Ariba, Concur) is supported. Use must be within the documented API controls and rate limits.

Customer-Owned Code (Customer Namespaces)

Custom RFCs, BAPIs, function modules, and OData services built in the customer namespace are not restricted. However, any calls from custom code to SAP's own APIs must still comply with the policy.

Undocumented SAP APIs - not supported or endorsed

SAP-internal APIs not listed on the SAP Business Accelerator or in product Documentation have always been used at the customer's own risk. SAP's stability and support obligations do not apply to undocumented APIs.

Unpermitted APIs

These are APIs explicitly flagged by an SAP Note, ATC checks as not-permitted, are indicated as "Confidential/Proprietary", or discovered only via debugging or reverse engineering. **ODP-RFC** is a concrete example where an SAP Note classifies it as unpermitted for customer or partner use

ODP-RFC is the only unpermitted interface so far

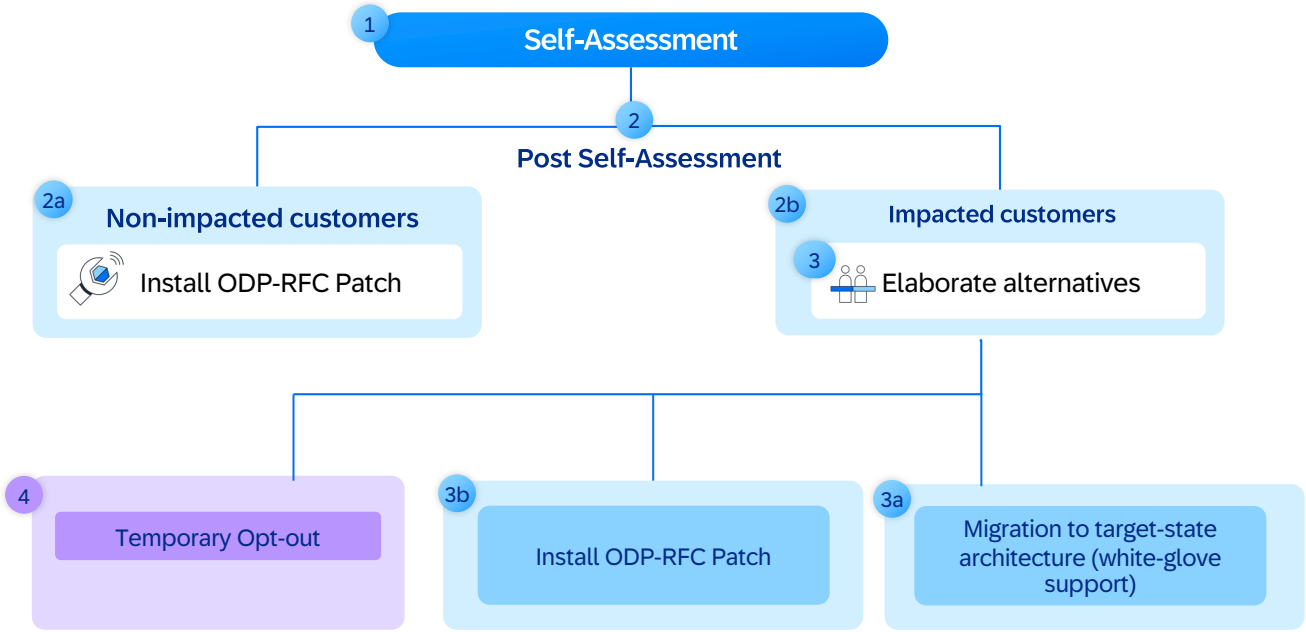
Phased ODP-RFC Rollout

1. Self-assessment tool shipped as SAP note enables customers to determine if impacted or not[1]

2. Post Self-Assessment:
   - 2a **Non-impacted customers** (those not using ODP-RFC for 3rd party egress), install ODP-RFC Security Patch immediately after shipment on June 9th
   - 2b **Impacted customers** (those using ODP-RFC for 3rd party egress) reach out to SAP contacts to elaborate alternatives

3. Impacted customers:
   - 3a **Transition Period:** Migration from ODP-RFC to the target-state architecture
   - 3b **After Planning future target architecture:** Install ODP-RFC Patch

4. **Temporary Opt-out**: suspension feature for ODP-RFC Patch available until December 31, 2026



[1] Please note that the above report does not provide conclusive results of the non-existence of unpermitted calls to the ODP-RFC interface.

Endorsed Architectures

A2A and MCP

A Primer

MCP (Model Context Protocol)

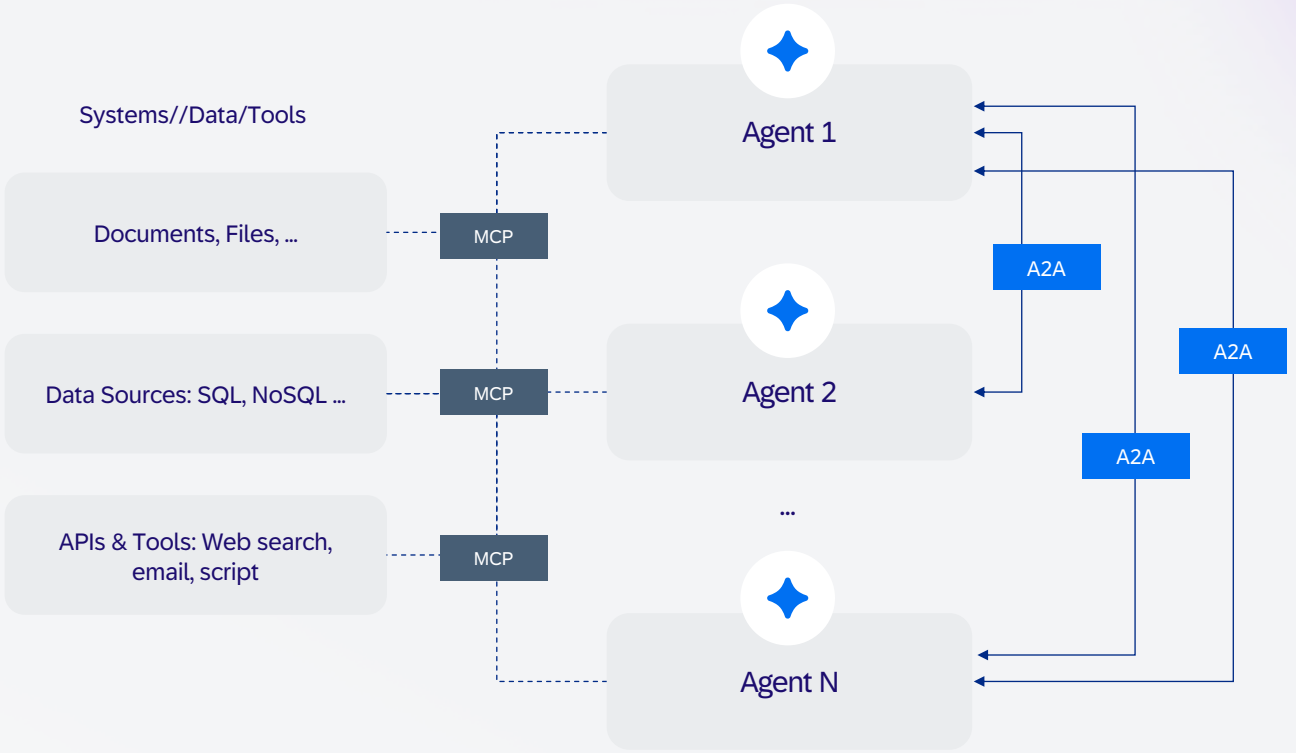
Connects AI agents to systems and data

- One integration works across any AI model or vendor
- Agents can connect to systems, documents, APIs, enterprise data, etc. as **tools**
- Eliminates fragmented, custom-built integrations

A2A (Agent2Agent Protocol)

Allows AI agents to collaborate across systems

- Multiple Agents can work together on complex tasks
- No vendor lock-in, agents from different providers can work together seamlessly
- End-to-end automation across business functions



Standardization

Key for Enterprise Adoption of Agentic AI

March 2025

Agent2Agent (Linux Foundation)
Release of Version 1.0

December 2025

Agentic AI Foundation (AAIF)
MCP Protocol | AGENTS.md | Goose

Founding Member

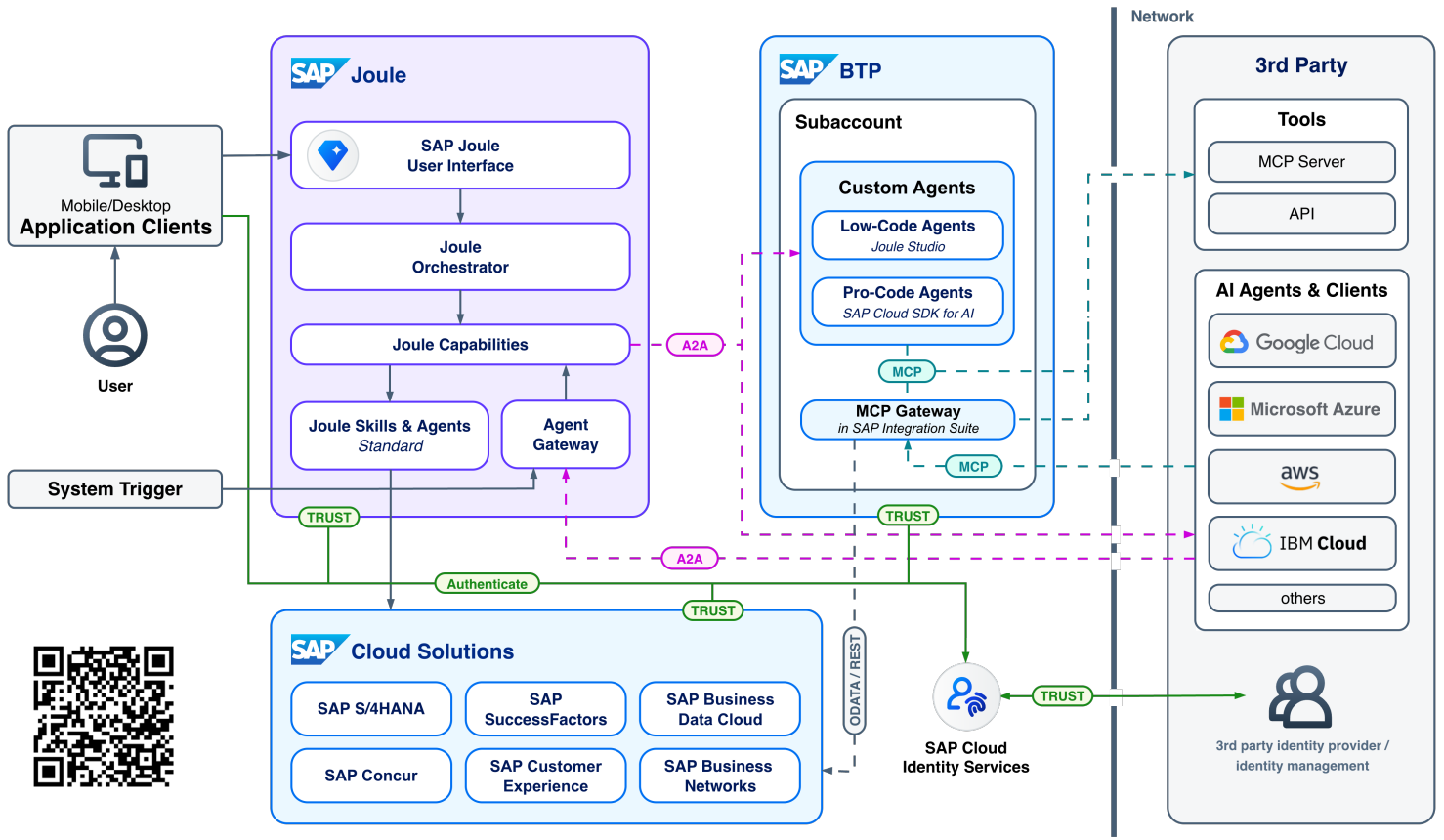
Member of the
Technical Steering Committee

Gold Member

Member of the Working Groups:
Identity & Trust (Co-Chair)
Observability & Traceability
Workflows & Process Integration

Agentic AI Architectures

AI Golden Path provides a guide to developing, deploying and managing AI agents in your SAP ecosystem. It details the architectural patterns, components and best practices for building both low-code and pro-code agents, integrating them with Joule through bidirectional A2A communication and ensuring seamless interoperability across the enterprise landscape.



Detailed Reference Architectures:

- A2A and MCP for Interoperability
- Low-Code AI Agents with Joule Studio
- Extend Joule with Joule Studio
- Pro-Code AI Agents on SAP BTP
- Integrating AI Agents with Joule
- Integrating Joule Agents into Your Ecosystem
- Third-Party MCP Access to SAP Solutions

Integration Suite:
from APIs to governed MCP servers

Introducing MCP Gateway in SAP Integration Suite

Your APIs, integrations, and data sources, exposed as governed, compliant MCP Servers (tools, resources, prompts any AI agent can consume.

CONNECT

Turn APIs and services into discoverable, reusable tools for agent use

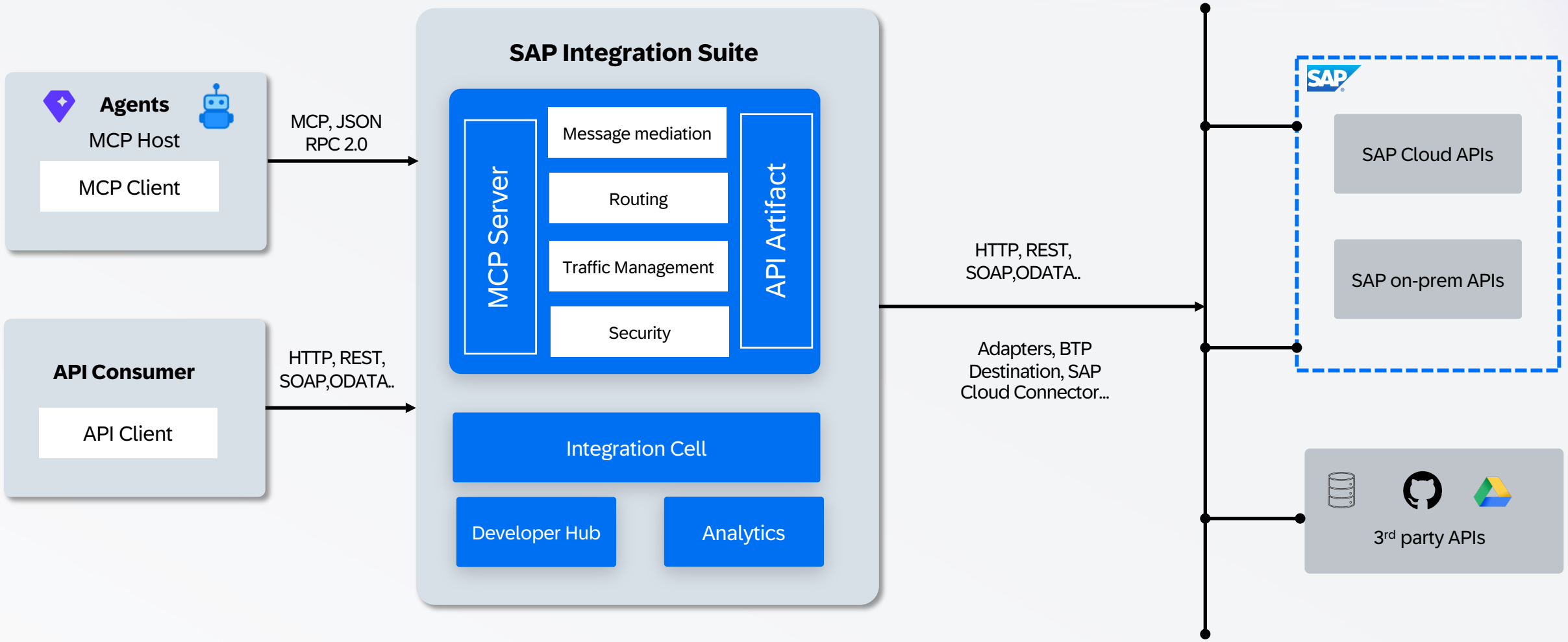
GOVERN

Apply policies, authentication, and usage controls to for agents to access tools and systems

ANALYZE

Provide visibility and traceability across agents, tools, and enterprise landscapes

MCP Gateway in SAP Integration Suite in a nutshell



Create

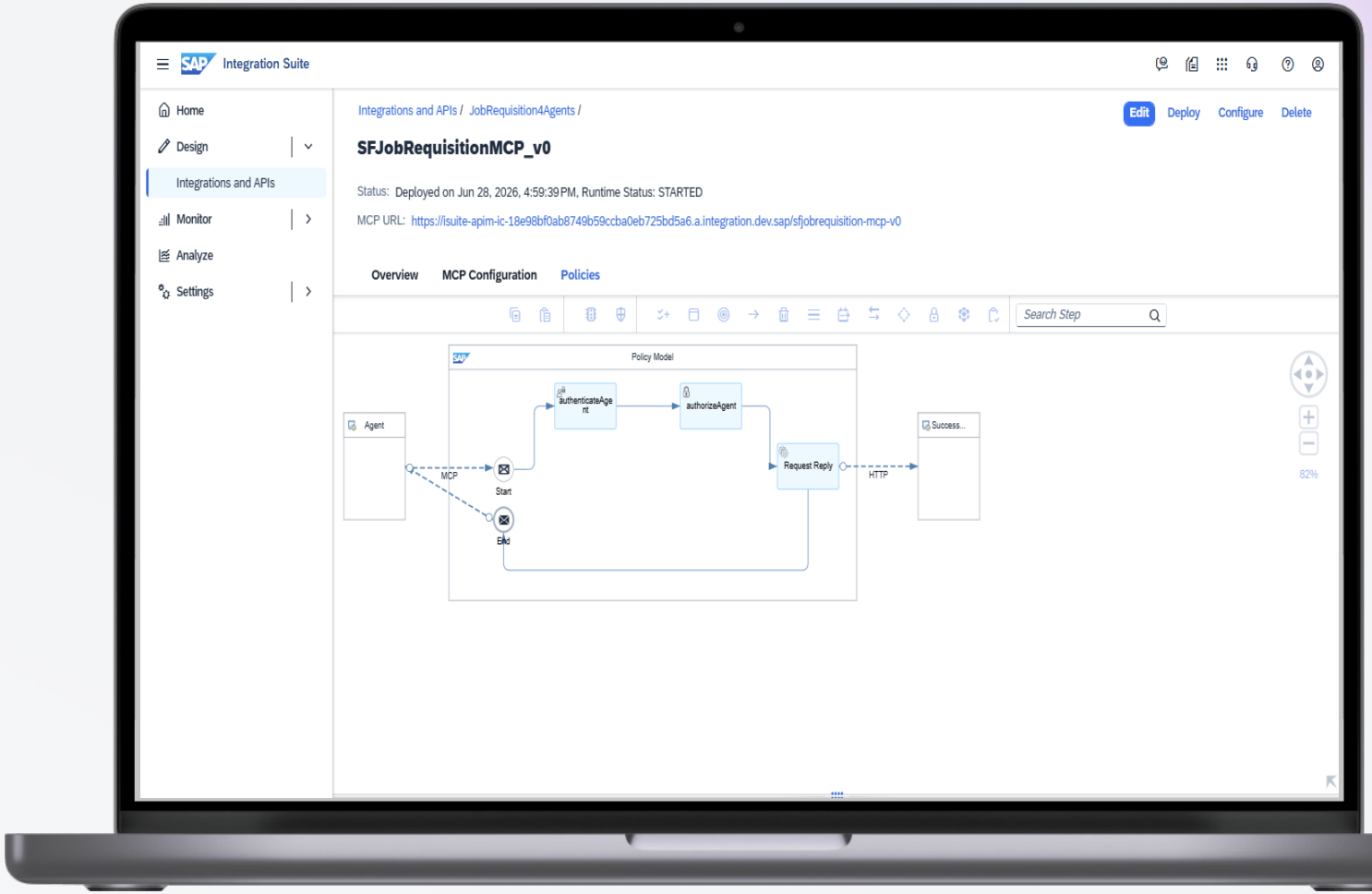
Expose APIs as MCP servers

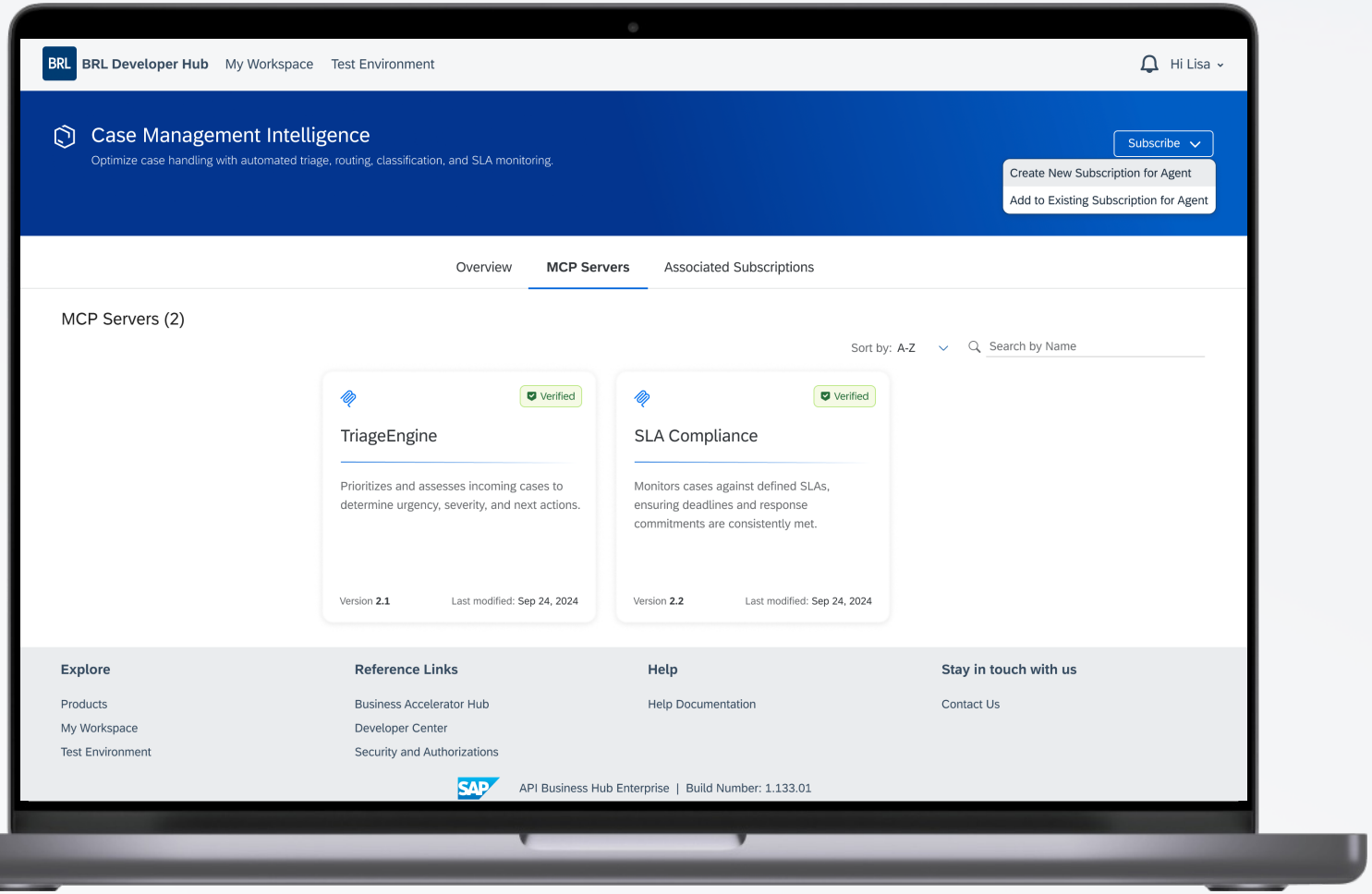
Extend existing API & integration investments for agent use by exposing SAP and third-party APIs as MCP servers

Shape APIs into agent-ready MCP tools by simplifying and packaging the right operations for agentic scenarios

Secure and Manage Traffic to MCP Servers from the AI Agents

Manage a **standardized connection layer** for agents across **SAP and third-party systems** within MCP servers via 250+ connectors





Govern

Apply Enterprise Controls across Design-time and runtime

Apply enterprise runtime guardrails
to enforce usage controls and protect backend systems

Centralize MCP servers in Developer Hub
to enable developers to discover MCP servers and tools for agent use

Register your agent and subscribe
to get scoped credential access to consume MCP servers

Enable secure production consumption
to ensure governed MCP servers are subscribed to and consumed in a controlled way

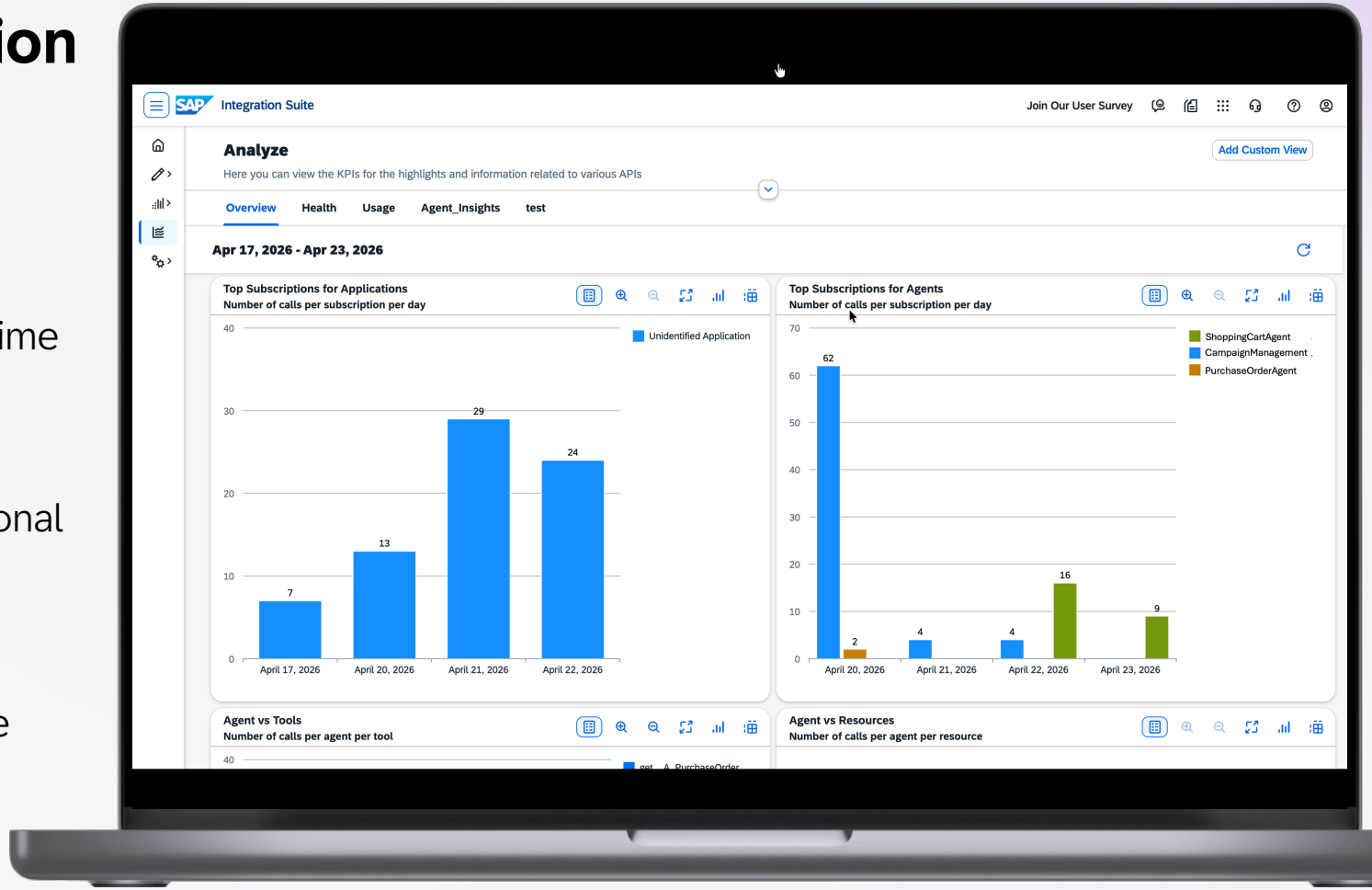
Observe

Monitor MCP usage in production

Track MCP activity across environments to understand how MCP servers are being used at runtime

Enable logging and traceability to support troubleshooting, auditability, and operational control

Improve operational visibility and usage insights at scale to help ensure reliable MCP usage across enterprise scenarios



Features and benefits of MCP Gateway

Multitude of paths to create MCP Server:

- Natively from an API Artifact
- Specifications of APIs from existing API Management deployments, external deployments
- RFC from ECC / S/4HANA
- Federate external MCP Servers*

Enterprise-Grade Security and Traffic Management:

Rate limiting, IP blocking, AuthNZ based on OIDC (SAP and 3rd Party), Payload protection

Agent ready Tools:

Technical specifications are translated to MCP schema, augmented with natural language semantics

API Composition and Optimization*:

Combine multiple backend APIs and expose them as optimized MCP endpoints for efficient agent consumption

Actionable Intelligent Insights:

Monitor and analyze MCP usage with comprehensive logs, traces, and intelligent analytics

Developer Engagement and Governance:

Foster collaboration, ensure compliance, and drive MCP adoption through robust governance and developer engagement tools

Unlock additional data sources *:

Heterogeneous data sources (databases, 250+ connectors), can be exposed as MCP tools and resources for streamlined access

Monetize Your Tools *:

Unlock new revenue streams by leveraging API management capabilities to create, manage, and sell MCP Tools

Shield from complexity:

MCP is still evolving rapidly. Running self-managed MCP servers means one must monitor the specification roadmap closely and plan for upgrade cycles. SAP-managed MCP infrastructure absorbs this complexity on your behalf.

** Roadmap item*

Joule Studio:
MCP in the agent-building experience

Joule Studio: MCP in the agent-building experience

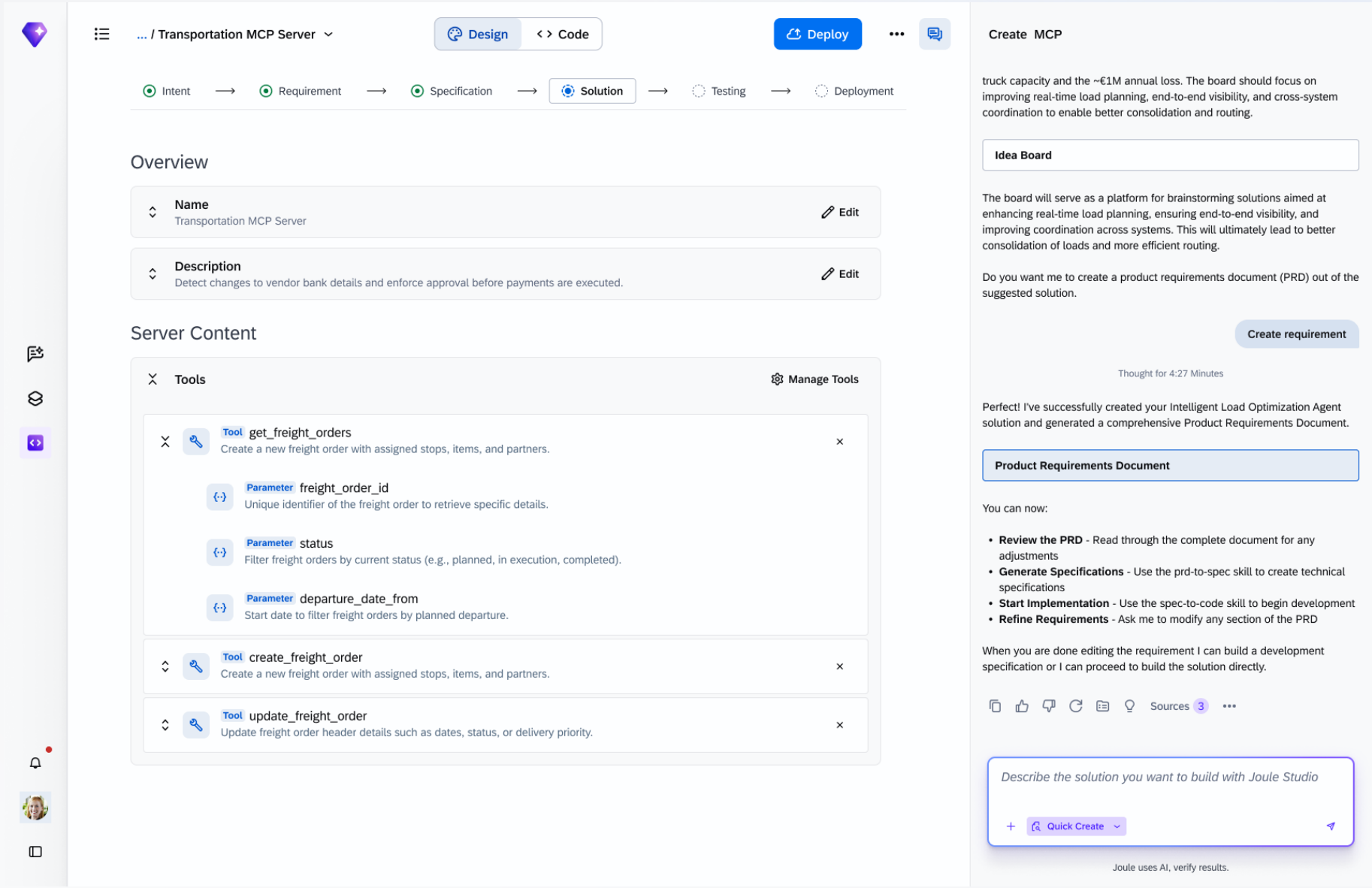
Accelerate with SAP-provided MCP servers

- Accelerate time to value with no custom build effort
- Leverage MCP servers optimized for SAP systems and scenarios
- Get started quickly with ready-to-use tools and skills

Innovate with custom MCP extensibility

- Build MCP servers around your specific business needs
- Tailor agent access to the processes that matter most
- Support differentiated requirements with purpose-built MCP tools

MCP in the agent-building experience: Joule Studio



More Information

API Policy FAQ Document

https://www.sap.com/documents/2026/04/e2a0665e-4c7f-0010-bca6-c68f7e60039b.html

AI Golden Path

https://architecture.learning.sap.com/docs/aigp

SAP Architecture Center

https://architecture.learning.sap.com/docs/ref-arch

AI-Native North Star Architecture

https://architecture.learning.sap.com/docs/nsa

FAQ – Top Questions

Q: What are the primary objectives of the SAP API Policy?

The API Policy has two core objectives: protecting platform stability and security, especially with the rise of AI and automation, and providing a harmonized framework for how APIs are intended to be used across the SAP portfolio. It does **not** mandate a specific SAP software solution.

See SAP API Policy FAQ, Q1

Q: Does the API Policy force customers to use only SAP-controlled AI platforms like Joule?

No. Customers can use **any third-party AI platform**, provided it connects to SAP through an endorsed architecture leveraging open protocols like **A2A and MCP**. SAP is a standards contributor to both protocols under the Linux Foundation.

See SAP API Policy FAQ, Q35, Q36, Q41

Q: Will rate limits and other protective measures cause existing integrations to suddenly fail?

No. Existing integrations using APIs for their documented purpose are not expected to be impacted, and SAP's approach prioritizes **dialogue first** - reviewing the use case with the customer before taking any restrictive measures. There are no automatic blocks or penalty models.

See SAP API Policy FAQ, Q10, Q11, Q19

Q: Does the API Policy invalidate customer-developed custom code in the customer namespace?

No. Customer-developed code in their own namespace remains permitted. However, compliance is determined by the **underlying SAP components the code calls** — custom code cannot be used to circumvent the policy's technical controls or to access SAP-internal interfaces.

See SAP API Policy FAQ, Q26, Q27, Q31

Q: Is it allowed to use non-published SAP function modules?

Using non-published SAP interfaces has always been **"at the customer's own risk"**, outside SAP's stability and support guarantees. The policy does not retroactively invalidate all such integrations, but SAP will provide notice if a specific interface presents a high risk - **ODP-RFC** being the concrete example of an explicitly prohibited interface for certain types of use.

See SAP API Policy FAQ, Q23, Q24

FAQ Document

https://www.sap.com/documents/2026/04/e2a0665e-4c7f-0010-bca6-c68f7e60039b.html

Thank you.

Contact information: