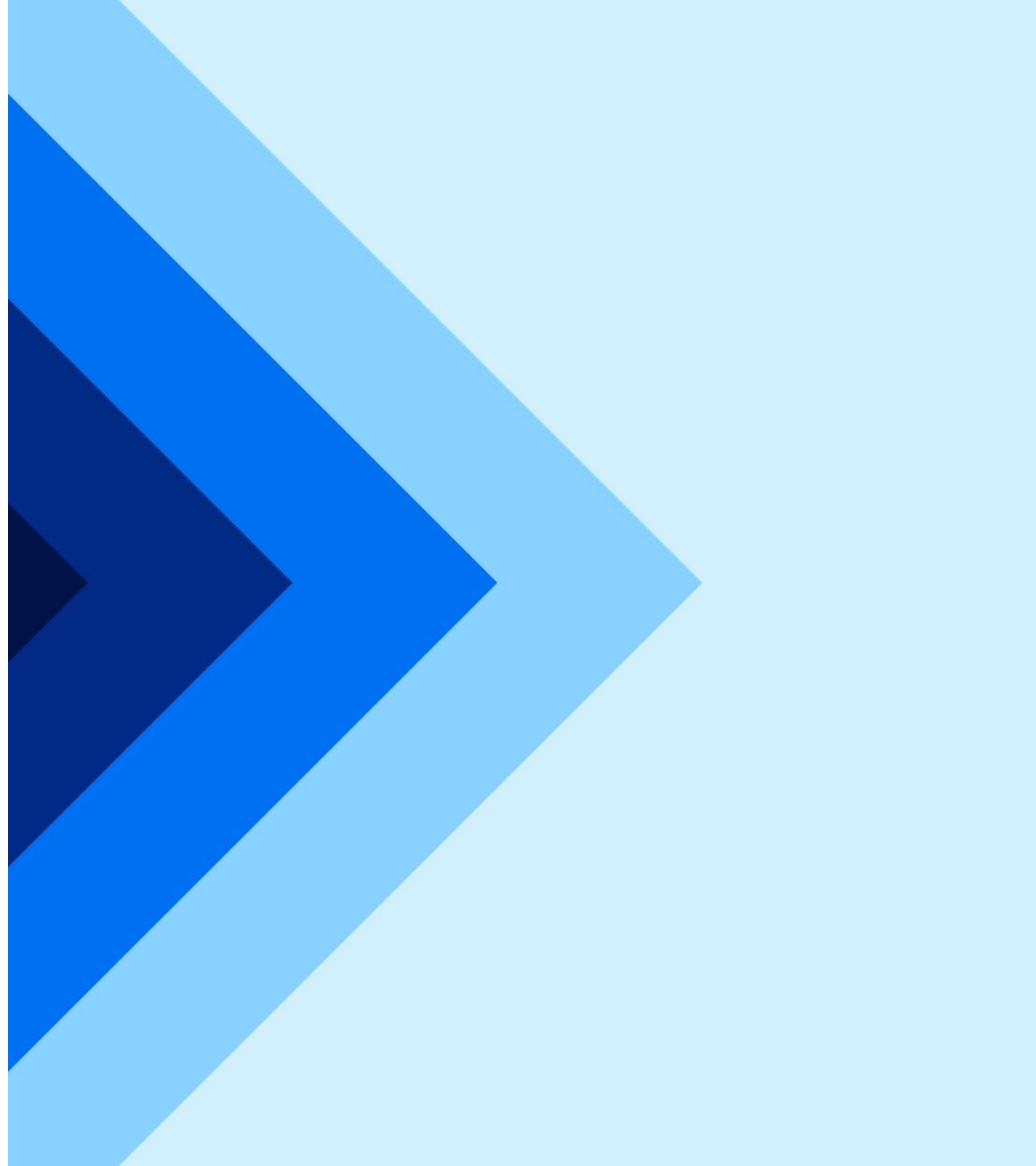




New SAP API policy

Eero Koskinen, SAP
BTP / BAIP Solution Advisor (but think of me as a technical architect)



**Best customer summary so far I've
ran into: "So SAP is preventing
other customers from doing silly
things which we wouldn't do
anyways"**

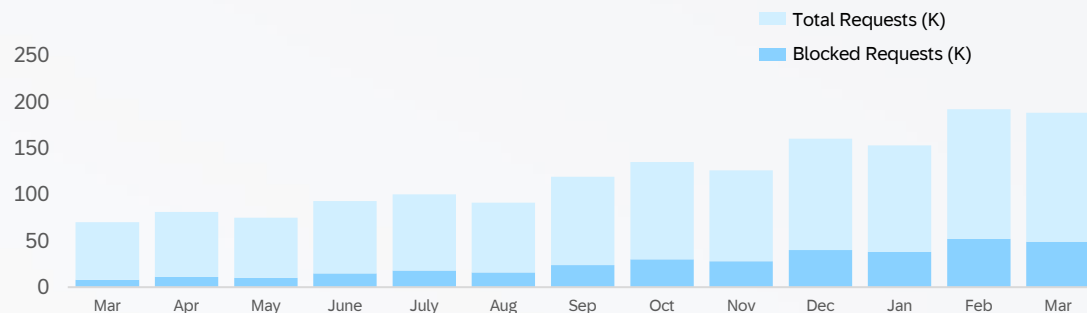
Recognize What Is Already Happening

Three 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 legacy controls 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 at machine speed.
- **New Attack Surface Through AI Tooling:** Direct agent connectivity creates significant risk. Without formal governance and technical guardrails, vulnerabilities like the OWASP Top 10 for [LLMs](#) and [MCPs](#) pose a major threat to system integrity.
- Transitioning to an endorsed architecture is critical to prevent AI innovation from destabilizing the business core.

Structured Data

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



Unstructured Data

AI bots hitting unstructured data sources arrive in **concentrated surges** tied to training and grounding cycles.



API Policy (and the agentic context)

WHAT | Building the right infrastructure for an open ecosystem

1 Fair and secure service access for our customers

API Policy

- **API Policy and FAQ** published on **April 27, 2026**
- **Outlines terms for:** API Availability, Limits, API Use, and Monitoring
- **Enforces** usage of Published APIs and adherence to Documentation on SAP Help and product developer portals

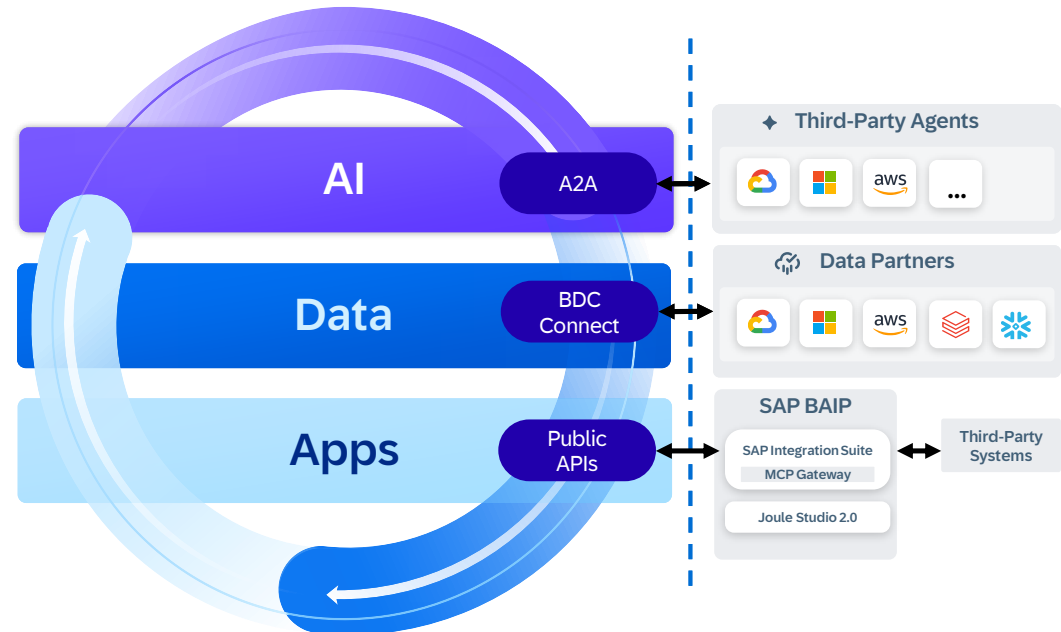
Industry-Standard API Protection & Fair Use

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



API Policy:

https://help.sap.com/doc/sap-api-policy/latest/en-US/API_Policy_latest.pdf

2. API CONTROLS

The following Specific and General Controls apply to API use (collectively, “API Controls”):

2.1. **Specific API Controls.** SAP documents and maintains specific API controls in the applicable product-specific Documentation or API Hub for each API, including:

- functional / technical use rate limits and quotas,
- deprecation schedules,
- data ingress/egress quotas,
- limits and preconditions for bulk extraction / replication, and
- other security/technical requirements.

2.2. **General API Controls**

2.2.1. SAP prohibits any API use for purposes of: (a) competitive analysis, (b) enabling functions or scenarios that are not part of the Documented Use unless otherwise authorized by SAP, or (c) in a manner that creates a risk to system performance, stability, or security.

2.2.2. Except through and within the limits of SAP-endorsed architectures, data services, or service-specific pathways expressly identified and intended for such purposes, SAP prohibits API use for: (a) interaction or integration with (semi-) autonomous or generative AI systems that plan, select, or execute sequences of API calls, and (b) scraping, harvesting, or systematic and/or large-scale data extraction or replication.

Data Access Strategy | SAP strengthens how data is accessed so customers can innovate with AI confidently while preserving data integrity and quality

What Customers Are Experiencing

As organizations scale AI and automation, data is accessed by more systems, tools, and agents than ever before. Without clear guardrails, this can impact data quality, agents' accuracy, security, and system reliability.

Our Commitment

SAP is strengthening how data is accessed so customers can

- Innovate with AI confidently
- Preserve data integrity and quality
- Maintain visibility and control over data usage

How We Do This in the Cloud

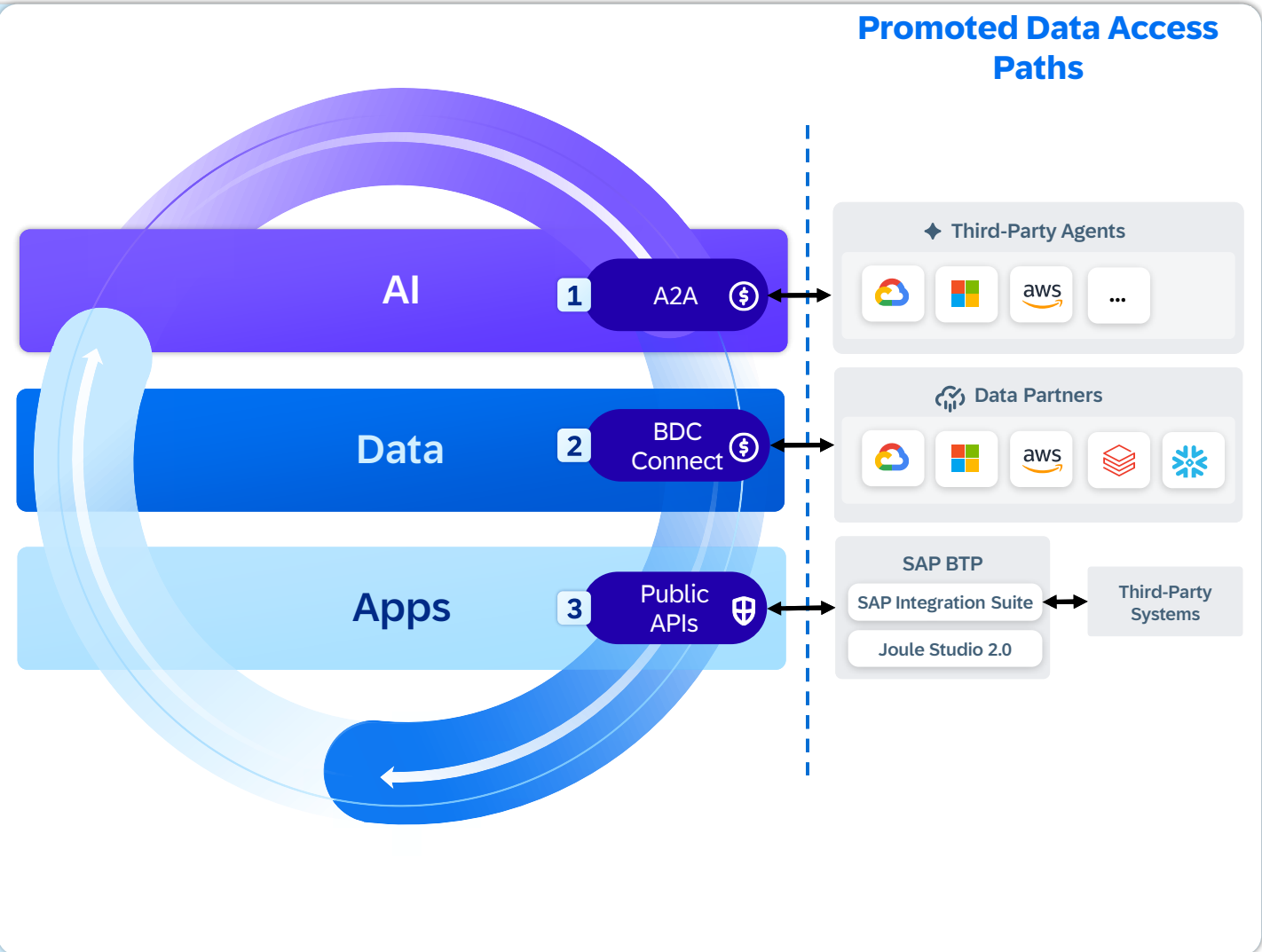
We provide clear, promoted paths for different needs

- 1 **AI automation:** secure agent-to-agent interaction
- 2 **Analytics & AI:** governed data access through SAP Business Data Cloud
- 3 **Integrations & extensions:** stable, documented public APIs

These approaches ensure data is used intentionally, transparently, and responsibly

What This Means for Customer

- Greater trust in your data foundation
- Predictable, scalable AI and analytics
- Long-term protection of data value



WHY | We're entering a new world of enterprise software with Data & AI

Motivation for API Policy: The cloud software market is on the advent of major **changes in the software ecosystem** that are strongly **AI- and data-forward**. The API policies enable our solutions to **deliver on SAP's promise** and **value to our customers** as the software ecosystem evolves into the next generation of enterprise capabilities.

1 Fair and secure service access for all our customers

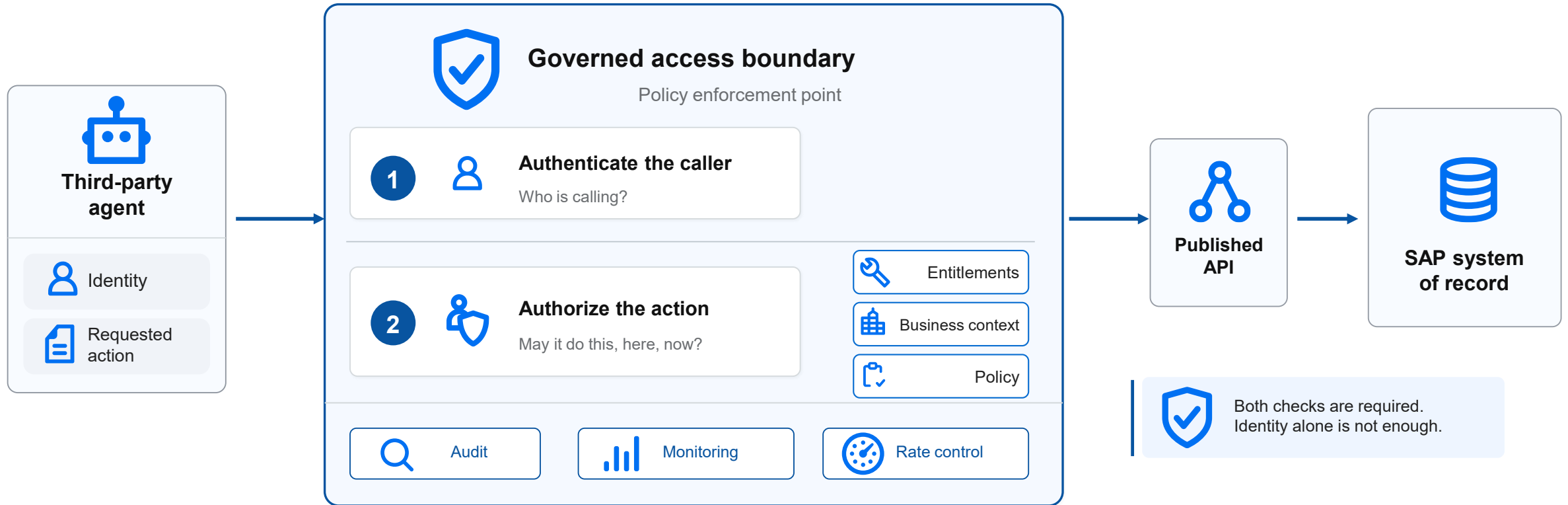
- Customers should have **access to** services that are **consistent, stable, and secure**
- By **avoiding ungoverned AI access** to SAP APIs, customers **realize value** from SAP solutions with **reduced risk of disruption**
- **Compliant interface** usage empowers customers to **innovate faster** in the context of their licensed Business Suite solutions

2 Fit-for-purpose, secure solutions for building AI-native applications

- Providing **clear architectural guidelines** on **contextual, governed data** strategies empowers customers with SAP's APIs
- **Clarity on data egress** with SAP's ecosystem strategy ensures a governed approach for customer access & security
- **AI Agent-to-Agent framework** helps ensure relevant, **reliable, AI with full context**

Advantage of API Policy: Governed API policy incl. essential **protections against ungoverned & unauthorized agentic access** will **benefit customers & partners**.

WHY | Agentic access requires a governed trust boundary



Equitable, stable service
for every customer



Reliable, contextual AI
with appropriately scoped access

HOW | API Policy legal framework and narrative

API Availability

Published APIs:

On the **SAP Business Accelerator Hub** or in **SAP product Documentation**; 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
- 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

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.

Monitoring

SAP monitors API usage to support compliance and platform stability

API Policy | What this means for our customers

SAP is standardizing API protections to help customers scale integrations and AI safely.

Stable and Reliable Use Case Specific APIs

- Well documented **APIs outlining intended fit for purpose** use cases
- **Stable APIs** with consistent safeguards to **protect performance** and **availability** for intended use cases

Right Path for Every Workload

- APIs for integrations and extensions using published APIs
- Governed data access for large-scale analytics and AI
- Secure, authorized interaction patterns for agent-to-agent and automated use cases.

Predictable Performance, Based on Data

- APIs designed to protect existing, well-designed integrations.
- API limits are data-driven, not arbitrary.
- API limits set individually per product / API based on historical usage to match real-world needs.

Equitable Access for Everyone

- Controls that are designed to promote equitable service quality across customers
- Industry-standard protections without changing how existing integrations work.

The API Policy **does not change existing customer functional entitlements** – it allows us to **continue to modernize** so that customers can scale integrations, analytics, and AI **securely, predictably, and responsibly**.

SAP's 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 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

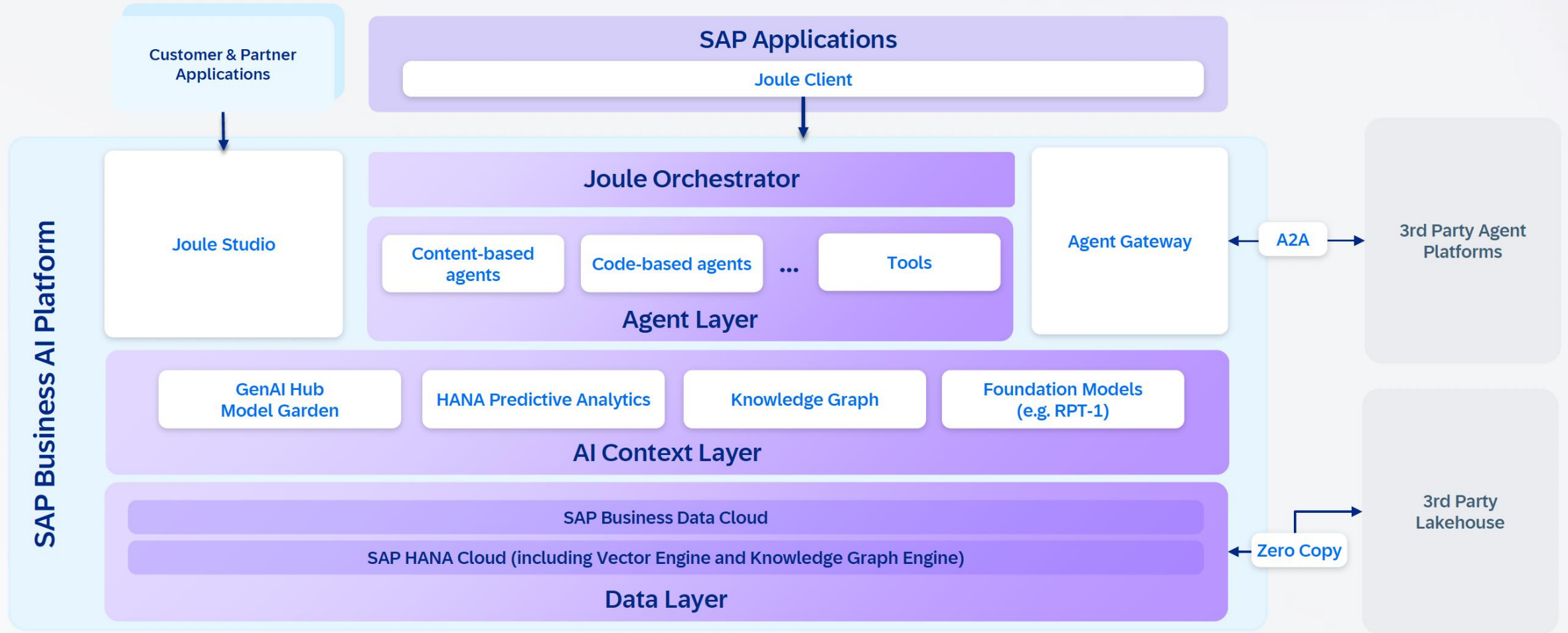
These are APIs explicitly flagged by an SAP Note, ATC checks as not-permitted, are indicated as "Confidential/Proprietary", or discovered only via debugging or reverse engineering. ODP-RFC is a concrete example where an [SAP Note](#) classifies it as unpermitted for customer or partner use

Endorsed architectures



AI Golden Path

Building AI-Native Outcomes



MCP Gateway: Endorsed pathway for Agents to access SAP APIs

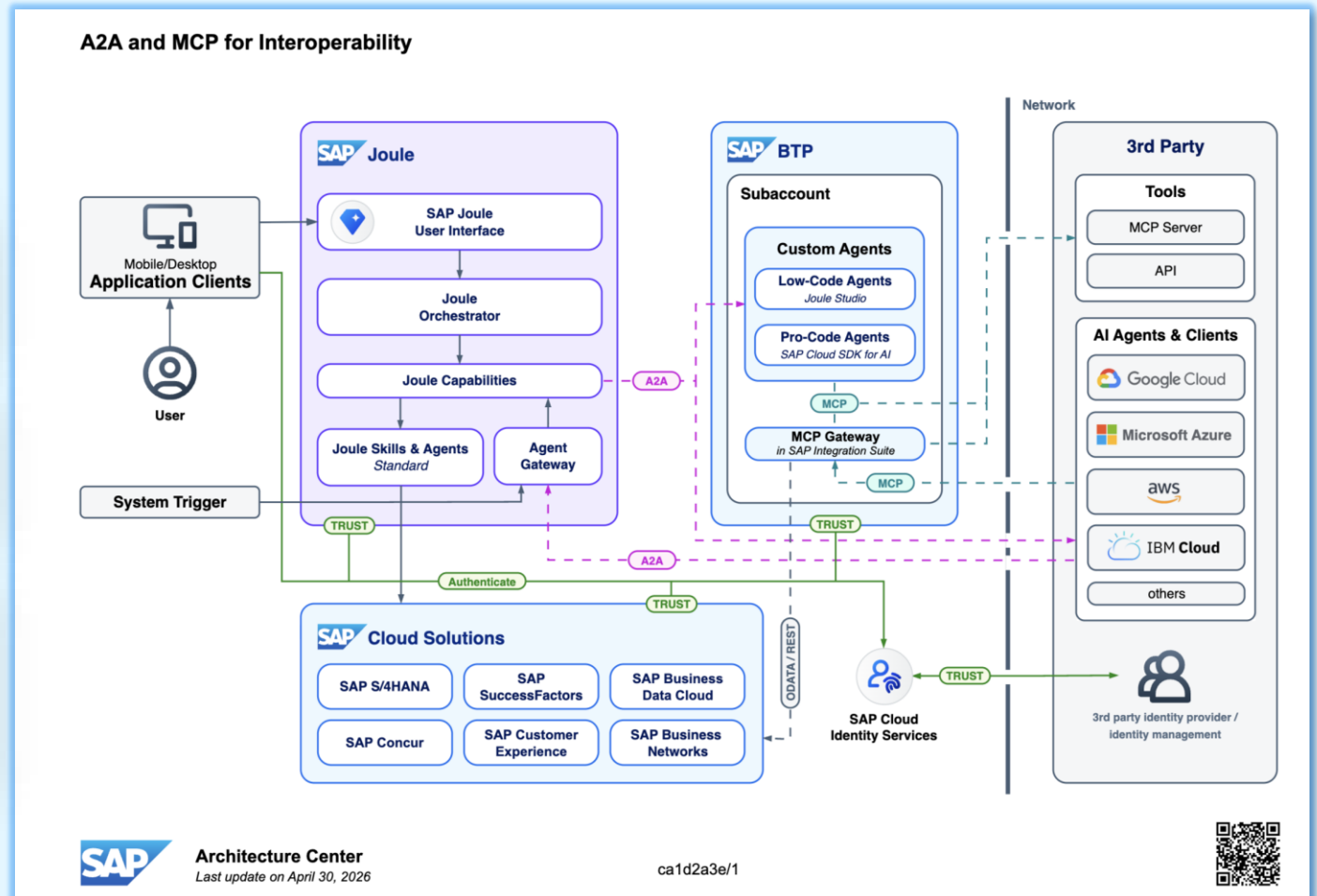
MCP Gateway is an endorsed pathway in SAP Architecture Center's reference architecture page

Recommendation Summary

External 3rd party Agents should use MCP Gateway to access SAP systems

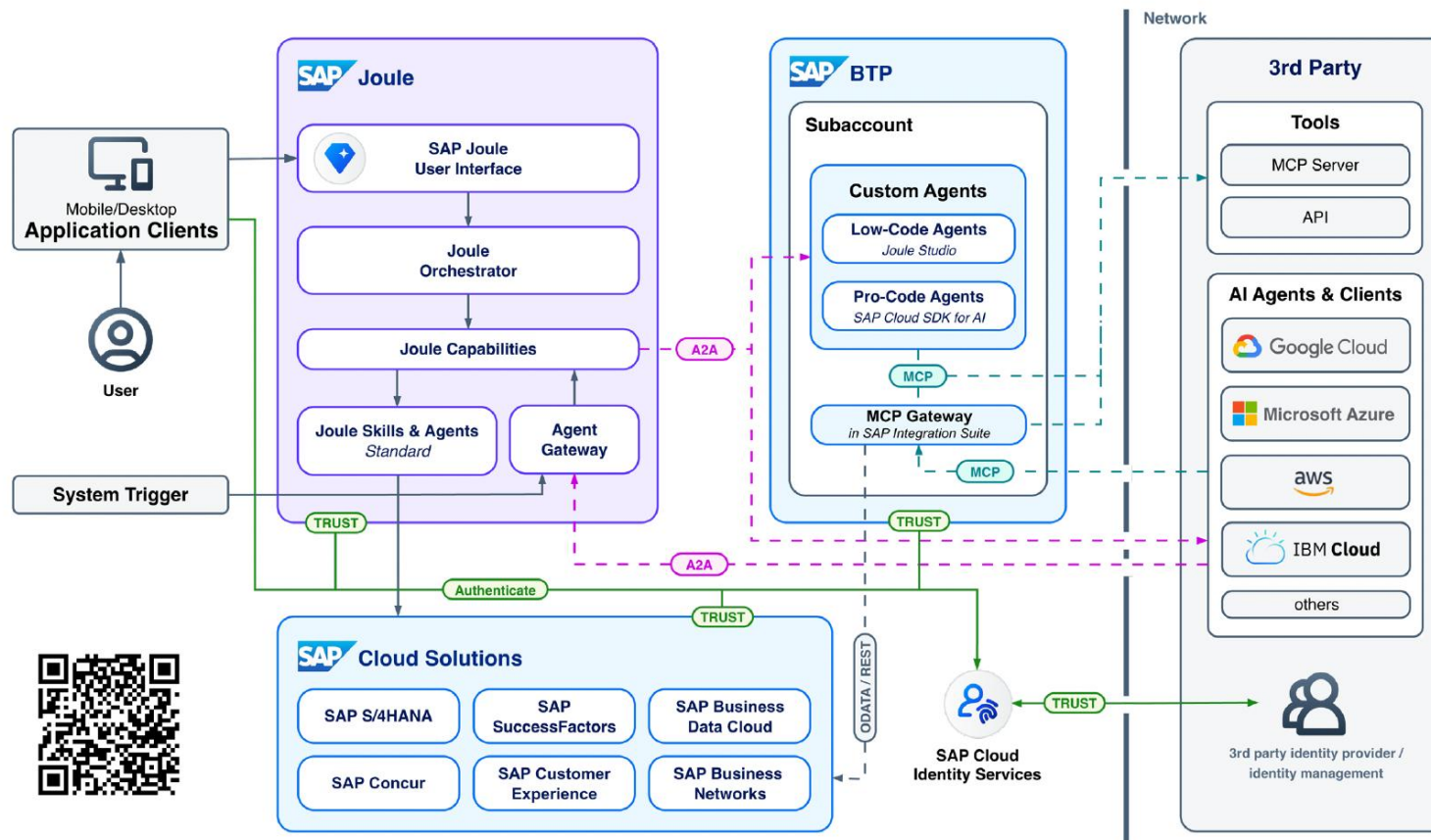
3rd party MCP Servers should federate with MCP Gateway to access SAP Systems (*on roadmap)

Customer-managed pro-code and low code Agents deployed in SAP BTP context should use MCP Gateway to access SAP systems



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.

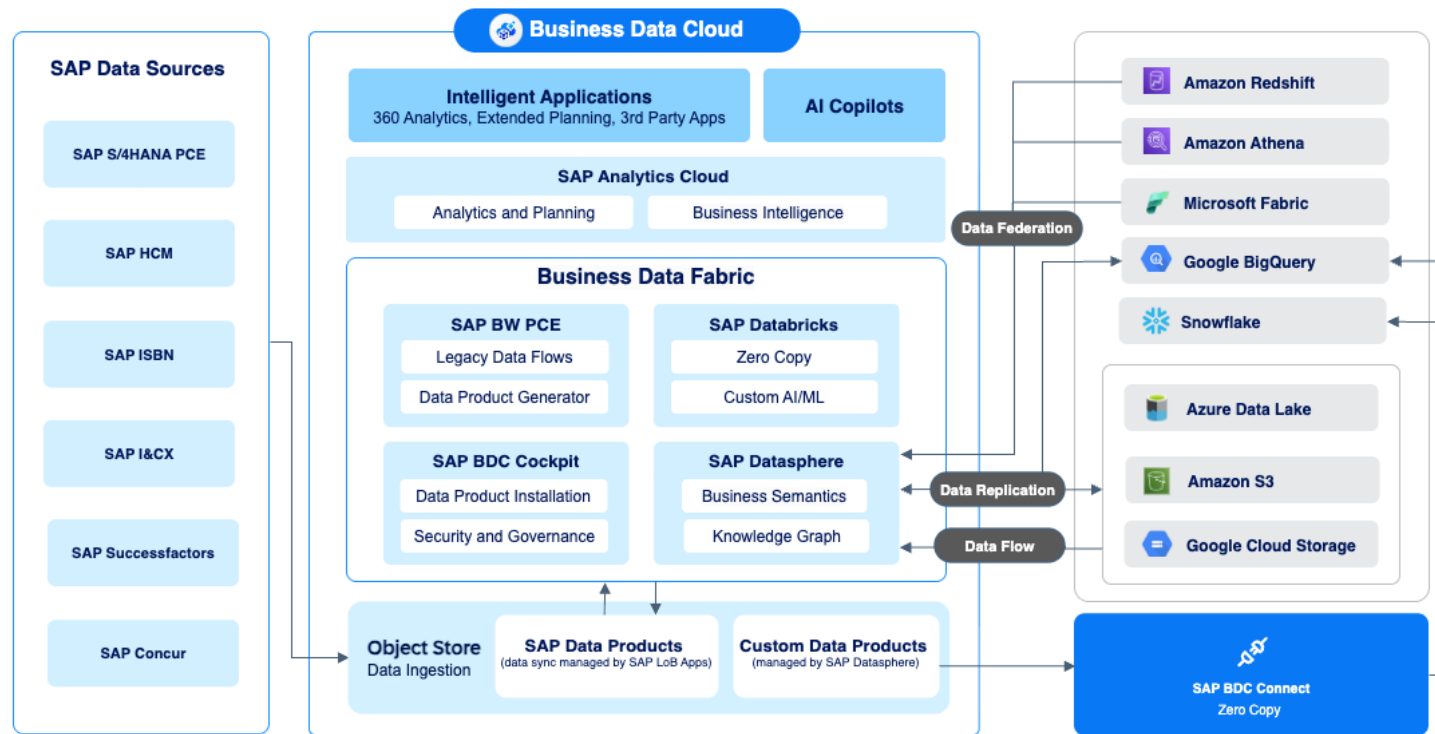


Detailed Reference Architectures:

- [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](#)

Data Architectures

The reference architecture outlines how to integrate data from SAP and non-SAP sources using SAP Business Data Cloud.



SAP Source Integration Options:

- Business Data from SAP applications are brought into the Object Store Layer of Business Data Cloud in the form of Data Products, enabling secured governed access of SAP data
- SAP Business Data Cloud also allows these systems to be connected natively using direct connections available in the SAP Datasphere layer for remote or replicated data access

Non-SAP (hyperscaler) Data Source Integration Options:

- BDC Connect / Delta Sharing integration
- Data Federation - SAP Datasphere
- Replication Flows - SAP Datasphere
- Data Flows - SAP Datasphere

Integration Categorized by Sources:

- [Integration with Databricks](#)
- [Integration with Snowflake](#)
- [Integration with Google Cloud Platform Sources](#)
- [Integration with Azure data sources](#)
- [Integration with AWS sources](#)

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>



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>



A Unified API Policy Built for the Agentic Era

Approach

A harmonized API governance framework that requires endorsed architectures for AI agents and automated traffic to ensure long term platform stability, security, and responsible AI innovation for every customer.

1 Protect Every Customer's Access Equitably and Without Disruption

- **Guarantee consistency:** ungoverned AI traffic creates unpredictable load spikes that degrade service reliability for every customer on the platform
- **Accelerate innovation:** compliant interface usage unlocks stable, predictable API surfaces that teams can build on

2 Fit-for-purpose, secure solutions for building AI-native applications

- Clear architectural guidelines on governed data strategies and data egress ensure secure, compliant use of SAP's APIs
- **Deploy with confidence:** a reliable, governed foundation accelerates the path from AI prototype to real-world business value

What's Changing

Route AI agents and automations through governed, secure pathways.



What's NOT Changing

Your existing licenses and entitlements are not changing. Your integrations that are in line with the Documentation and the Agreement will work exactly as before.



Why This Matters

A single uncontrolled AI agent can trigger thousands of API calls from one prompt — risking system stability and data security for every user on the platform.





Additional slides, if time allows

Architecture center

<https://architecture.learning.sap.com/docs/ref-arch/137800>

Filters

58 unique documents found ⓘ

AI & Machine Learning (32) ▾

SAP AI Agent Hub

Generative AI on SAP BTP

Transforming Enterprise Data Strategy with SAP Business Data Cloud

Integrating and Extending Joule

Embodied AI Agents & Robotics

Agentic AI & AI Agents ▾

A2A and MCP for Interoperability

Building AI Agents with Joule Studio

Custom Pro-Code AI Agents on SAP BTP

Integrating AI Agents with Joule

Integrating Joule Agents into Your Ecosystem

Agent Identity

Agentic Engineering for SAP Extensions

Agent Behavior Mining

Third-Party MCP Access ▾

Microsoft Copilot Studio and the MCP Gateway in SAP Integration Suite

SAP Document AI

Application Dev. & Automation (29) ▾

Designing Event-Driven Applications

Establish a central entry point with SAP Build Work Zone

Integrating and Extending Joule

Embodied AI Agents & Robotics

Agentic AI & AI Agents ▾

A2A and MCP for Interoperability

Building AI Agents with Joule Studio

Custom Pro-Code AI Agents on SAP BTP

Integrating AI Agents with Joule

Integrating Joule Agents into Your Ecosystem

Agentic Engineering for SAP Extensions

Third-Party MCP Access ▾

⚠ Customer Responsibility

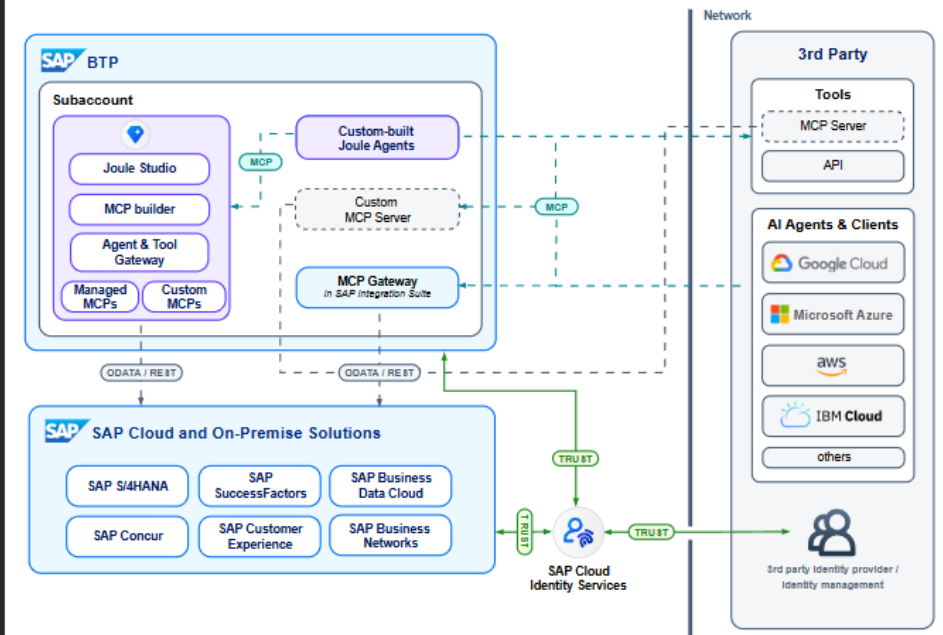
Customers and partners may use third-party MCP servers to access SAP APIs, **provided the following conditions are met: the SAP API Policy is adhered to in full**, in particular the section on General API Controls; authentication and authorization are enforced on every connection as described below; rate limits of the underlying SAP APIs are respected; and infrastructure stability and security hardening as described on this page are in place. The operational responsibility for third-party MCP servers, including their security posture, availability, upgrade compatibility and compliance, rests entirely with the customer or partner deploying it.

⚠ Protocol Volatility

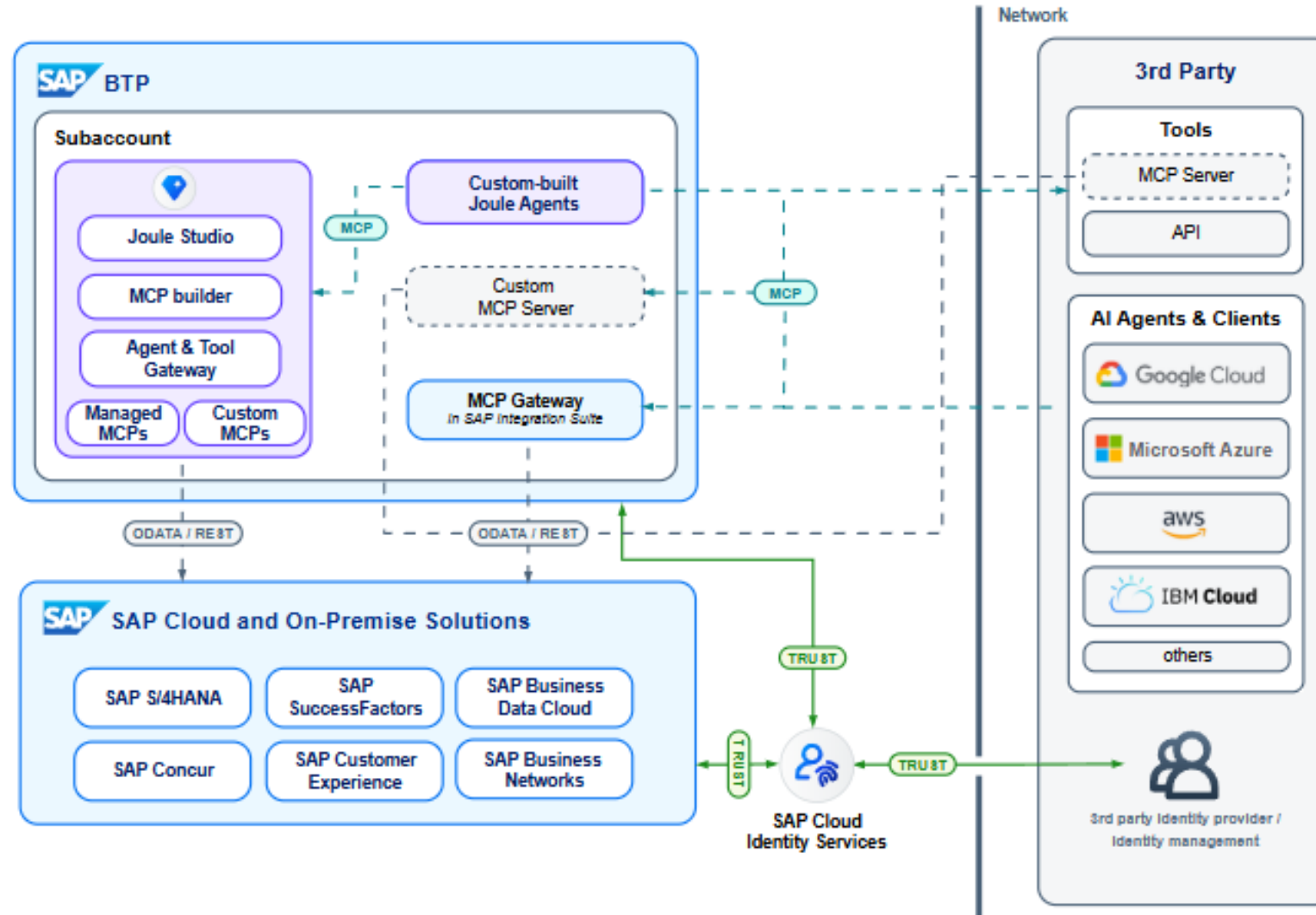
MCP is still evolving rapidly. A release candidate for a major revision of the MCP specification introduces breaking changes. Customers or partners running self-managed MCP servers must monitor the specification roadmap closely and plan for upgrade cycles. SAP-managed MCP infrastructure absorbs this complexity on your behalf.

Architecture

Third-Party MCP Access to SAP Solutions



Third-Party MCP Access to SAP Solutions



Architecture Center
Last update on June 8, 2026

137800



Microsoft specifically on SAP Architecture Center

architecture.learning.sap.com/docs/ref-arch/d2e34e

SAP Fiori Launchpad SAPpilaista ilm Priva (14) WhatsApp AI SAPpilaista uusi

Copilot Studio with MCP Gateway in SAP Integration Suite

Agents Generative AI Microsoft Azure

Last updated on Jun 18, 2026 by hobru

Disclaimer

The [Agent Gateway](#) is not yet generally available (GA). The outlined architecture here shows ways how the integration with Copilot Studio and SAP can be done today.

Microsoft Copilot Studio is Microsoft's low-code platform for building and orchestrating AI agents across Microsoft 365, Teams, and custom channels.

If you are new to Copilot Studio, start with the official product documentation: [Microsoft Copilot Studio documentation](#).

Through the **Model Context Protocol (MCP)**, a Copilot Studio agent can discover and invoke SAP business capabilities as governed tools — without bespoke point-to-point integration code and without moving SAP data out of its system of record.

In this pattern, Copilot Studio acts as the **MCP client**, and the **MCP Gateway in SAP Integration Suite** acts as the governed entry point that exposes SAP APIs, integration flows, and data sources as MCP-compliant tools. Identity flows end-to-end through a trust relationship between **Microsoft Entra ID** and **SAP Cloud Identity Services**, so every tool call runs in the context of the signed-in business user and respects existing SAP authorizations.

Microsoft Copilot Studio and the MCP Gateway in SAP Integration Suite

The diagram illustrates the architecture for integrating Microsoft Copilot Studio with SAP Integration Suite via the Model Context Protocol (MCP). It is divided into three main sections: SAP BTP, SAP Cloud and On-Premise Solutions, and Microsoft Azure.

- SAP BTP (Subaccount):** Contains components like Joule Studio, MCP builder, Agent & Tool Gateway, Managed MCPs, and Custom MCPs. It also includes Custom-built Joule Agents and the MCP Gateway in SAP Integration Suite.
- SAP Cloud and On-Premise Solutions:** Includes SAP S/4HANA, SAP SuccessFactors, and SAP Business Data Cloud. These are connected to the SAP BTP subaccount via ODATA / REST interfaces.
- Microsoft Azure:** Contains Azure API Management (MCP Server, API), Microsoft AI (Microsoft Azure, Microsoft AI Foundry, Copilot Studio, and others). The MCP Gateway in SAP Integration Suite acts as the MCP client, connecting to the MCP Server in Azure API Management.

The diagram shows the flow of data and control through the MCP and the MCP Gateway in SAP Integration Suite, enabling Copilot Studio to interact with SAP business capabilities.

And same in Microsoft documentation.

<https://learn.microsoft.com/en-us/azure/sap/microsoft-ai/copilot-studio/architecture-mcp-gateway-integration-suite>

The screenshot shows the Microsoft Ignite 2026 website. The header includes the event name, dates (November 17–20, 2026), and a 'Register now' button. The navigation bar features the Microsoft logo, 'Learn', and various categories like Documentation, Training & Labs, Q&A, and Topics. Below this, there's a secondary navigation bar with 'Azure' and sub-categories like Products, Architecture, Migration, Develop, Learn Azure, Troubleshooting, and Resources. The main content area displays the article title 'Use the SAP MCP Gateway on SAP Integration Suite' with a breadcrumb trail 'Learn > Azure > SAP on Azure'. A sidebar on the left contains a search bar and a list of related topics, with 'Using the SAP MCP Gateway on SAP Integration Suite' highlighted. The article content includes a 'Note' box stating that this is a documented and approved SAP reference architecture, and a section titled 'Why use this scenario?' explaining the benefits of the Model Context Protocol (MCP) for AI agents.

Microsoft Ignite
November 17–20, 2026
Register now >

Learn | Documentation | Training & Labs | Q&A | Topics

Azure | Products | Architecture | Migration | Develop | Learn Azure | Troubleshooting | Resources

Learn > Azure > SAP on Azure > Ask Learn

Use the SAP MCP Gateway on SAP Integration Suite

Find by title

- SAP Joule and Microsoft Copilot
- Copilot Studio and SAP
 - Copilot Studio overview
 - Azure API Management and virtual network peering
 - On-premises data gateway with access to BAPIs, RFCs, and OData services
 - SAP Business Technology Platform with SAP API Management and SAP Cloud Connector
 - Using the SAP MCP Gateway on SAP Integration Suite**
 - Demo scenario (public SAP system)
- Copilot Studio and Security
- Foundry AI and SAP Overview

Download PDF

Summarize this article for me

Note

This integration is a documented and approved SAP reference architecture. For SAP's guidance on consuming SAP data and processes from AI agents through the Model Context Protocol, and specifically on connecting Microsoft Copilot Studio to the SAP MCP Gateway, see the SAP Architecture Center reference architectures [Third-Party MCP Access to SAP Solutions](#) and [Microsoft Copilot Studio and the MCP Gateway in SAP Integration Suite](#).

Why use this scenario?

The [Model Context Protocol \(MCP\)](#) is the standard way for AI agents to discover and call tools. Instead of wiring a Copilot to one fixed API at a time, an MCP based integration lets the agent dynamically discover the available SAP tools, understand their inputs and outputs, and build the correct request to retrieve or update data in the SAP system.

By using the **SAP MCP Gateway** - a capability of the **SAP Integration Suite** (running on the Integration Suite's edge / Integration Cell runtime) - SAP provides a **governed, SAP-managed**

Thank you.

