Third-Party Martech in SAP Environments:

An Architecture and Risk Assessment

Table of contents

About this document:

This is a structured technical and risk assessment, not a product brochure. It is written for CTOs, CIOs, IT Directors, and SAP Platform Owners at enterprise organizations already running SAP Customer Experience products. The intent is to give you the framing to evaluate your current architecture honestly — and to understand where a native SAP alternative changes the risk profile.

01 Risk Assessment Summary

Three categories of risk. All of them are probably live in your environment right now. Most of them aren't on anyone's radar.

If your organization runs SAP Customer Experience products and uses a third-party marketing platform — Salesforce Marketing Cloud, Braze, Klaviyo, Adobe Journey Optimizer, or any similar standalone tool — your environment is carrying three categories of IT risk that rarely surface in budget discussions or architecture reviews.

The first is integration debt. Every custom connector between a third-party marketing platform and your SAP environment is a liability. It breaks on API updates, SAP upgrades, and schema changes. The engineers who built it move on. The documentation ages. And the failure mode is a broken production workflow that someone discovers at the worst possible time.

The second is PII governance exposure. Customer behavioral data, contact records, purchase history, and consent preferences are flowing continuously out of your SAP environment into a vendor's infrastructure that you don't govern. That's a data residency question, a breach surface expansion, and a GDPR or CCPA audit exposure — every day the integration runs.

The third is compliance overhead. Each third-party marketing platform requires its own annual security review, its own vendor risk assessment, its own DPA. Those cycles run outside your established SAP governance cadence, require real legal and security resource, and compound year over year as your marketing stack grows.

This assessment covers each risk category in detail, gives you the architecture picture for the native alternative, and ends with a vendor consolidation framework you can use to run this evaluation internally — against your current platform or any future one.

The core findings

These three risk categories are structural consequences of running a customer engagement capability outside the SAP ecosystem. They are not configuration problems or process failures — they are architectural ones.

The structural response is to run the engagement capability inside the same infrastructure, identity model, and compliance framework already governing the rest of your SAP environment — which is what SAP Engagement Cloud does. Whether that is the right path for your organization depends on your current environment, contract status, and consolidation timeline. Section 07 gives you the framework to evaluate that honestly.

02 The Integration Debt Problem

Custom middleware in SAP environments: what breaks, who owns it, and what it actually costs.

The connector that nobody owns

When a third-party marketing platform gets integrated into an SAP environment, the integration is typically built as a project deliverable. Someone on the IT team — or a systems integrator — builds a connector. It gets tested, signed off, and handed to operations. Then the project closes and everyone moves on.

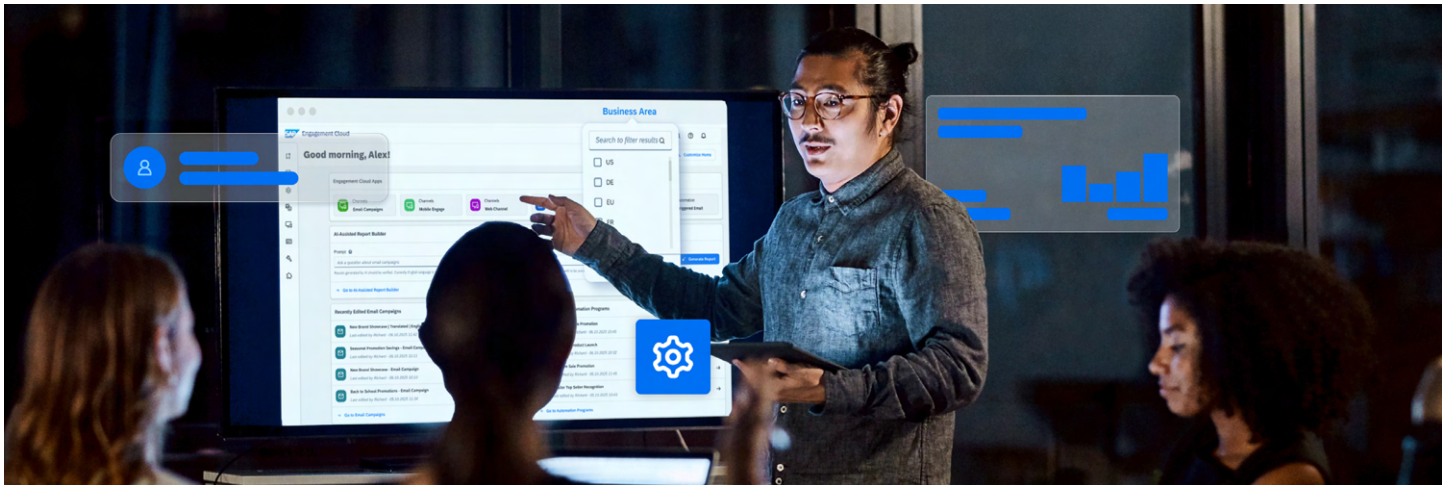
What doesn't move on is the integration. It stays in production, connecting a system your IT team governs to a vendor's infrastructure that it doesn't. And every time something changes on either side — a vendor API update, an SAP CRM upgrade, a new data model in S/4HANA, a change in the marketing platform's authentication requirements — someone on your team has to respond.

That someone is often unclear. The integration was built by a consultant who no longer has a contract. The internal engineer who understood it left eighteen months ago. The documentation is a six-page PDF from the original project. This is not an edge case. It's the standard operating condition for third-party marketing integrations in enterprise SAP environments.

39%

of IT team time is spent designing, building, and testing custom integrations between systems.

Deloitte Digital,
Connectivity Benchmark Report



What the failure modes look like

The integration maintenance cycle follows a predictable pattern. The connector runs fine until a change event occurs upstream or downstream. Common triggers:

Vendor API updates

The marketing platform vendor pushes a new API version. Your connector was built against the old one. The vendor deprecates the old endpoint. Data stops flowing. You find out when a marketing campaign fires blank personalization fields or doesn't fire at all.

SAP upgrade cycles

SAP conducts quarterly release updates. The OData service definitions change. The connector's field mapping breaks. You find out from a data sync error log that nobody was watching.

Schema changes

Marketing adds a new field they need in the platform. It doesn't exist in the integration mapping. Either the field doesn't flow through, or someone builds an ad hoc workaround that becomes the next undocumented dependency.

Authentication changes

The vendor rotates credentials or changes their OAuth implementation. The connector fails silently until someone notices that contact records haven't updated in three days.

The real cost of a custom marketing integration:

Initial build (3–6 months in complex SAP environments); ongoing maintenance (0.5–1.0 FTE equivalent annually); incident response averaging 2–4 times per year; and compounding technical debt as each system evolves independently. None of this appears in the platform license comparison that justified the original purchase.

When a connector fails in production, the recovery cycle typically runs 2–5 business days end-to-end: triage, root cause identification, fix development, testing across environments, and redeployment. During that window, the marketing platform is running on stale data — or not running at all.

Why this risk is systematically underreported

Integration maintenance cost almost never appears in a platform budget. The license fee is in marketing's budget. The engineering time maintaining the connector is in IT's headcount. The incident response cost is absorbed as operational overhead. Nobody runs a total cost calculation that combines them.

The result is that when marketing comes to IT to evaluate a new platform or renew an existing contract, the true carrying cost of the current architecture isn't part of the conversation. IT approves or flags the license renewal. Marketing renews. The integration debt continues accumulating invisibly.

03 PII and Data Governance Exposure

Customer data outside the SAP perimeter: residency, breach surface, and what auditors will ask.

Start with the audit question your team should be able to answer

If a regulator, enterprise customer, or internal auditor asks: “Where is customer PII flowing outside the SAP environment, and what governance controls exist on those flows?” — can your team answer that completely and accurately right now? If the answer requires going back to the marketing platform vendor to ask, that is the gap this section describes.

Every third-party marketing platform connected to your SAP environment requires a continuous outbound flow of personally identifiable information. Contact records. Behavioral signals from web and app interactions. Purchase history. Consent and preference data. Email engagement metrics tied to individual customer identities.

That data leaves your SAP environment — where you have governance controls, data residency policies, and audit trails — and enters a vendor’s infrastructure. In many cases, IT teams haven’t fully mapped this flow. They know the integration exists. They don’t always know exactly what data is moving, how often, where it’s landing, or how the vendor handles it downstream.

That gap matters. A lot.

Three specific exposures

Data residency: Where is your customer PII actually hosted? Most third-party marketing platforms offer data residency options — but the default is often a US-based data center, and most enterprise procurement processes don't verify this at contract signature. If your organization has EU customer data subject to GDPR, or has made data residency commitments to regulators or enterprise customers, the gap between your stated policy and the vendor's actual infrastructure is a live compliance risk.

Breach surface expansion: Every external system that holds copies of your customer PII is an additional breach vector. When you add a third-party marketing platform to your environment, you're extending your effective breach surface to include that vendor's entire infrastructure and all of their sub processors. If the vendor suffers a breach, your customers' data is involved. Your notification obligations apply. Your regulatory exposure applies. You may or may not have adequate visibility into what happened.

Data subject request fulfillment: Under GDPR, CCPA, and similar frameworks, when a customer requests deletion of their personal data, you're obligated to fulfill that request across all systems where their data exists. If your IT team can't guarantee that a deletion request propagates correctly from SAP through your third-party marketing platform and all its downstream systems, that's a compliance gap. Not a theoretical one — a real one that regulators and auditors will probe.

Checkpoint:
Before you continue

If your team can answer the opening question cleanly — you know exactly what PII is flowing, to which vendor, hosted in which region, under which DPA — the three exposures below are already managed. If any part of that answer is unclear, the sections below describe the specific risk categories and what they mean for your audit posture.

What the SAP-native model changes

With SAP Engagement Cloud, customer data does not leave the SAP perimeter. It is processed within SAP-managed cloud infrastructure, covered by SAP's data residency options, and governed under the same data processing framework as the rest of your SAP environment. Data residency is available in EU, US, and APAC regions — configured at deployment and documented at the SAP Trust Center. Your existing DPA with SAP covers it. Your existing data residency commitments apply to it. Data subject deletion requests flow through a system your team governs end-to-end.

The audit question above has a clean answer: all customer PII remains within the SAP infrastructure governed by your existing DPA, subject to your existing data residency configuration. No external vendor. No additional breach surface. No separate deletion workflow to maintain.

04 Compliance Overhead: The Recurring Cost Nobody Budgets For

Vendor review cycles, DPA management, and the governance gap that compounds every year.

The review cycle that runs parallel to everything else

Enterprise compliance governance for a third-party marketing platform doesn't end at contract signature. It's an annual cycle. Security posture review. Vendor risk assessment. DPA renewal — and if the vendor has changed their data processing practices, infrastructure, or sub processor list since last year, that renewal is a renegotiation, not a rubber stamp.

That cycle requires real resource. Legal reviews the updated DPA. Security reviews the vendor's latest SOC 2 or ISO certification. Procurement manages the renewal timeline. The relevant business owner validates the use case. In a mature enterprise compliance function, this process typically runs 6–8 weeks per vendor, per year — based on standard enterprise compliance practice. Your organization's actual cycle may vary depending on internal governance maturity and the vendor's documentation quality.

And it runs entirely outside your SAP governance cadence. It can't be absorbed into your existing SAP security review. It can't be tagged onto your SAP compliance calendar. It's a separate process, with separate owners, for a system that marketing selected and IT supports.

What this looks like across a marketing stack

Most enterprise marketing organizations don't run a single tool. They run a stack. A primary marketing automation platform. A CDP or data activation layer. An analytics or attribution tool. Possibly a loyalty platform. A personalization engine for the web layer. Each one is a separate vendor. Each one has PII. Each one requires its own annual compliance cycle. Run the math for your environment: how many third-party marketing or CX platforms currently have access to customer PII from your SAP systems? Multiply that by 6–8 weeks of cross-functional compliance resource per year. That's the overhead your organization is carrying — in legal, security, and procurement time — that nobody attributes to the marketing budget.

The governance consolidation case

SAP Engagement Cloud's compliance posture is documented at the SAP Trust Center and covered by your existing SAP DPA. Your security and legal teams already know how to review it. The annual compliance overhead for SAP Engagement Cloud is not additive — it's absorbed into the review cycle you already run for the rest of your SAP environment.

05 What a Customer Engagement Platform Actually Does

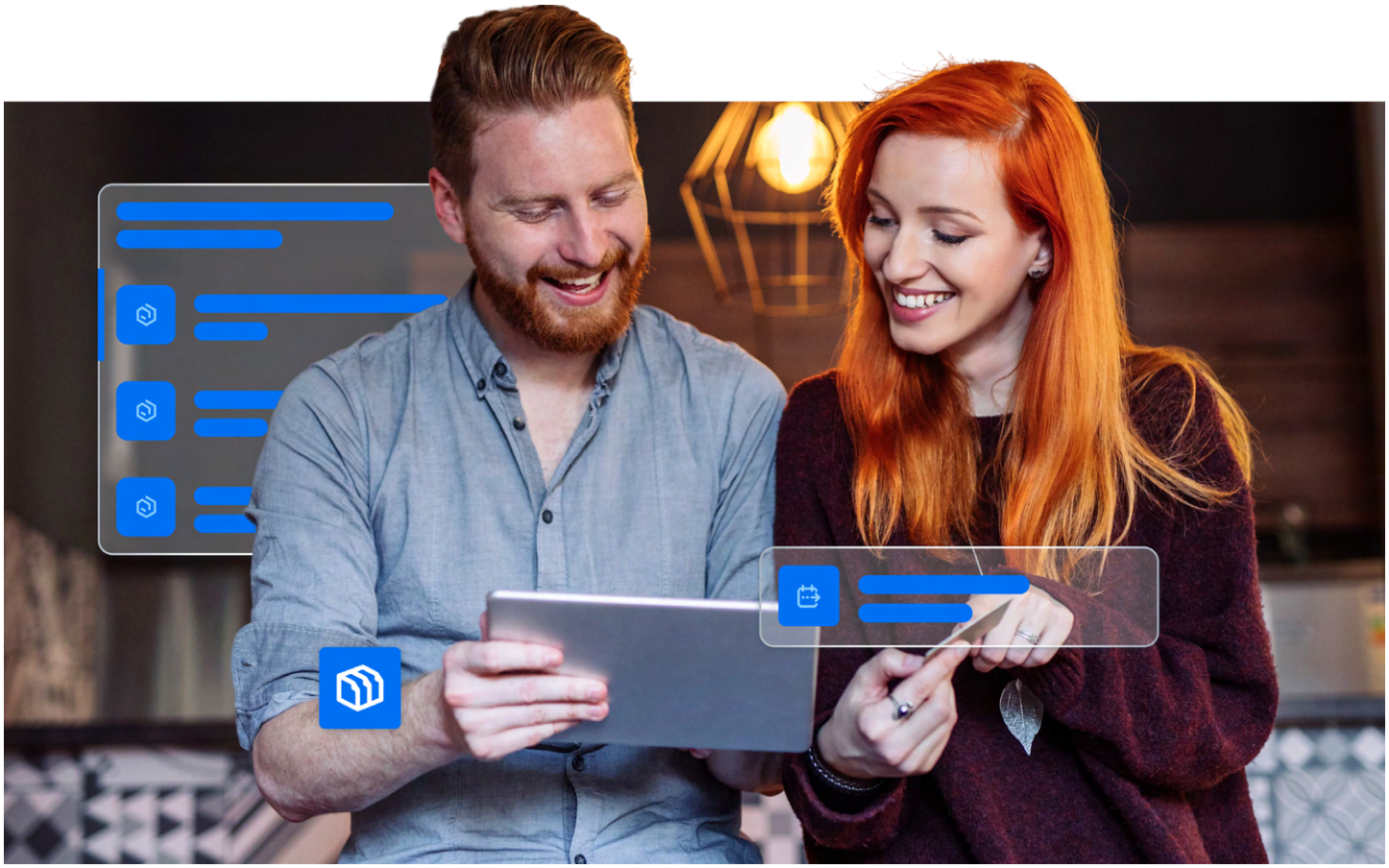
A technical definition for IT leaders who have not evaluated this product category before. If you already know what OData events, contact sync, and behavioral triggers feed into a marketing automation engine — skip to Section 06.

The operational definition

A customer engagement platform automates and personalizes how an organization communicates with customers at scale. It sits at the intersection of customer data and outbound communication channels — email, SMS, push notifications, in-app messages, personalized web experiences. And it handles a set of operational decisions continuously and automatically: which customers get a communication, what that communication contains, which channel it goes on, and when it arrives.

These decisions happen millions of times per day in a large enterprise. They can't be made manually. They require live connections to customer behavioral data, purchase history, CRM records, consent preferences, and segment definitions. The system making those decisions — whatever it is — is the customer engagement platform.

It's running in your environment right now, whether IT has been part of the conversation about it or not.



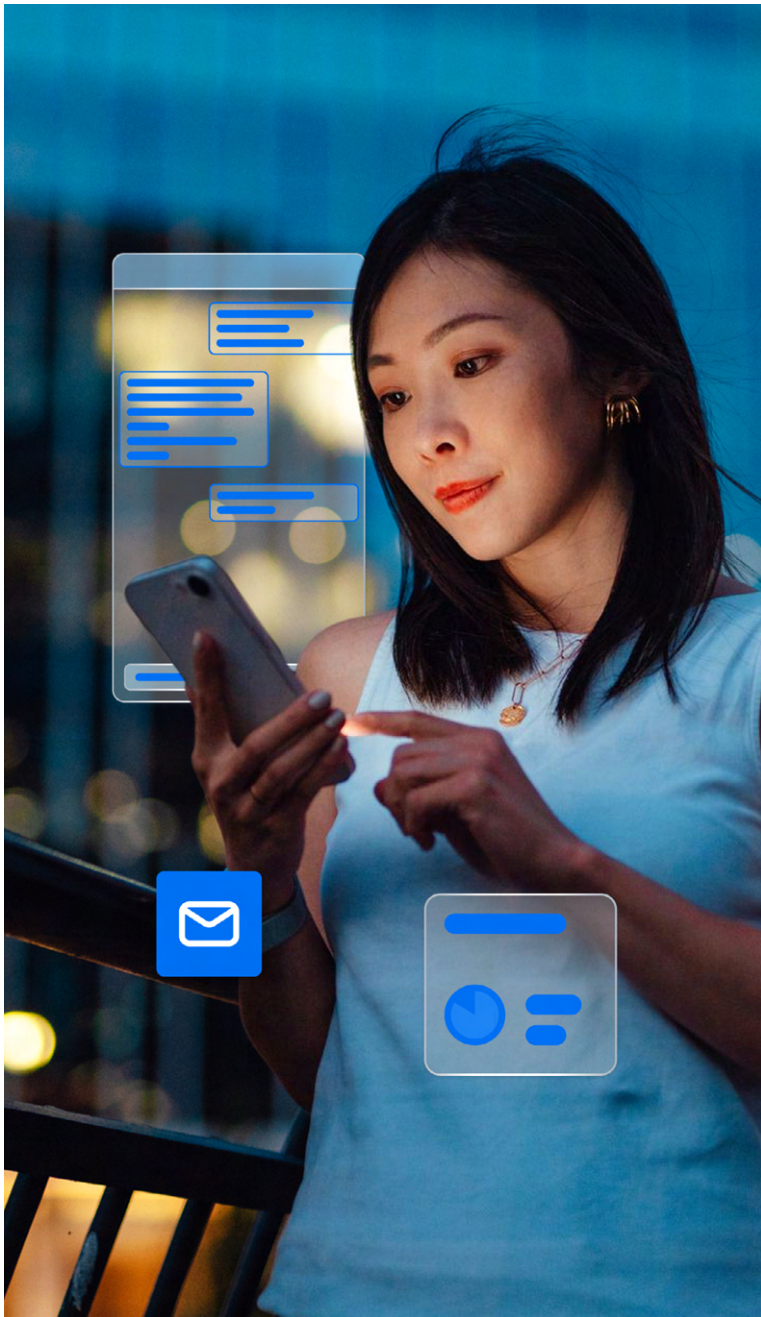
Capability	What it does	Data dependency
Omnichannel Automation	Triggers communications across email, SMS, push, and web based on customer events and lifecycle stage	Behavioral events, contact records, purchase history
AI Personalization	Predicts best content, send time, and channel per individual customer	Historical engagement data, purchase patterns, segment membership
Lifecycle Journey Orchestration	Automates multi-step engagement flows without custom code	CRM data, event triggers, consent records
Real-Time Segmentation	Builds and updates dynamic audience segments from live behavioral signals	CRM data, real-time behavioral stream
Revenue Attribution	Connects engagement activity to revenue outcomes at campaign and channel level	Transaction data, campaign performance, customer IDs

Why this is inherently an IT architecture question

Every data dependency in that table requires a live connection to systems IT governs. CRM records. Transaction data from commerce or ERP. Behavioral signals from web and app infrastructure. Consent data from identity and governance systems.

There's no version of customer engagement platform deployment that doesn't involve significant IT architecture decisions. The question isn't whether IT is involved. It's whether IT is at the table when the integration architecture is being designed — or called in after the platform is live to deal with what was built without them.

It's running in your environment right now, whether IT has been part of the conversation about it or not.



←

06 Architecture Assessment: SAP Engagement Cloud vs. Third-Party Alternatives

Where it sits in the stack, how it connects, and what's different about the native integration model.

Stack position

SAP Engagement Cloud is part of the SAP Customer Experience suite. It's not an external application that happens to have a connector for SAP. It's an SAP application that integrates within SAP's own managed integration architecture — positioned as the omnichannel engagement layer between your data infrastructure and your customer-facing channels.

Integration layer: SAP Integration Suite on BTP

The integration between SAP Engagement Cloud and the rest of your SAP environment runs through SAP Integration Suite on BTP — SAP's own managed integration layer. Contact synchronization with SAP Sales Cloud uses OData service connections through SAP Integration Suite iFlows. SAP Account Engagement handles out-of-the-box bidirectional sync for standard contact and account data. Extension scenarios — custom fields, non-standard objects — are handled through configurable Groovy-script iFlows within Integration Suite. These are configured by your integration team or SAP Professional Services using the same tooling and skills your team already applies to other SAP integrations. No separate middleware skillset required.

No third-party middleware. No custom connector outside your standard SAP operational model. The integration is built, managed, and maintained within the same tooling your team uses for other SAP integrations. When SAP pushes an update, the integration is SAP's problem to maintain — not yours.

Identity layer: SAP Cloud Identity Services

Authentication runs through SAP Cloud Identity Services — the same central IAM layer governing your broader SAP landscape. OpenID Connect and OAuth 2.0. SCIM-based provisioning for user lifecycle management. SSO across the SAP CX suite. No separate identity provider. No parallel user store. Your existing IAM governance model extends to cover SAP Engagement Cloud the same way it covers your other SAP applications.

Data governance and compliance

Customer data in SAP Engagement Cloud is hosted within SAP-managed cloud infrastructure, subject to SAP's data residency options and covered by the SAP Trust Center compliance posture. ISO/IEC 27001 certified. ISO/IEC 27035 for incident management. GDPR and CCPA compliance built in. If your organization is covered by SAP's enterprise DPA, that coverage extends to SAP Engagement Cloud. No incremental DPA negotiation. No new vendor legal review cycle.

Risk category	Third-party platform	SAP Engagement Cloud
Integration debt	Custom connector; 3–6 months to build; 0.5–1.0 FTE/yr to maintain	SAP Integration Suite iFlows; SAP-managed; no separate ownership
PII governance	Customer data leaves SAP perimeter; separate data residency controls needed	Stays within SAP infrastructure; existing DPA and residency apply
Breach surface	Third-party vendor infrastructure adds external exposure	No expansion of breach surface beyond existing SAP footprint
Compliance overhead	Annual independent security review and DPA renewal per vendor	Absorbed into existing SAP compliance cycle; SAP Trust Center
Identity management	Separate IdP or custom SSO implementation required	SAP Cloud Identity Services; no new infrastructure
Vendor relationship	New contract, new SLA, new escalation path	Single SAP vendor relationship covers full stack
Upgrade compatibility	Your team owns compatibility testing on every SAP upgrade	SAP owns compatibility between its own products

07 Vendor Consolidation Assessment Framework

Run this against any customer engagement platform — your current one or any future candidate.

This framework is designed to be applied to your existing marketing platform stack, not just to SAP Engagement Cloud. A platform that can't answer these questions cleanly is carrying hidden risk in your environment. Use these to structure your internal evaluation.

Integration architecture

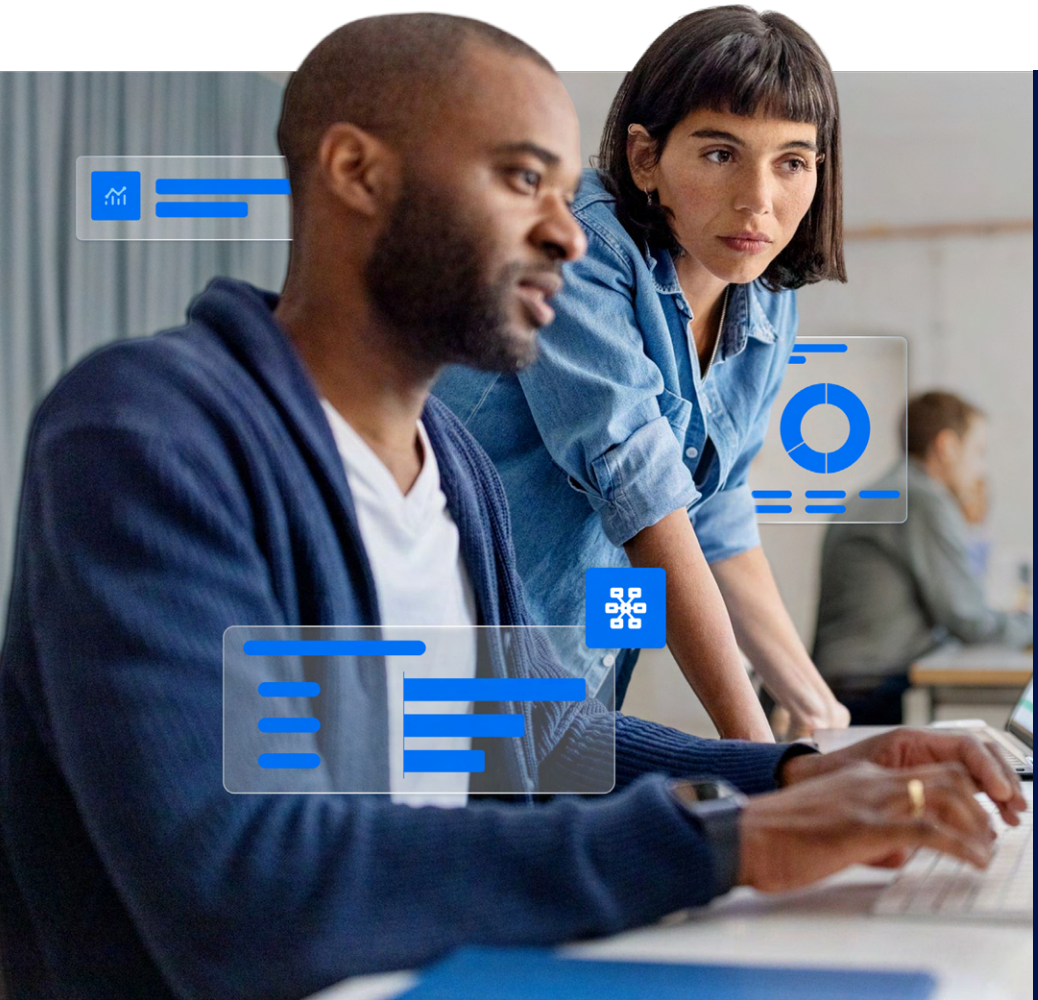
Integration layer	Does the integration run through SAP-managed infrastructure (SAP Integration Suite on BTP), or is it a custom connector your team owns and maintains outside normal SAP change management?
API change ownership	When the vendor updates their API, who owns the integration compatibility work? What's the SLA, and who absorbs the rework cost?
Data latency	Is the data connection real-time or batch? What's the actual lag between a customer event in SAP Sales and Service Cloud and its availability in the marketing platform?
Upgrade impact	When you upgrade SAP Sales Cloud or S/4HANA, what happens to this integration? Who tests it, and what does remediation look like?

PII governance and data residency

Integration layer	Does customer PII stay within the SAP governance perimeter, or does it leave the environment your team controls?
Residency verification	Where is customer data physically hosted? Have you verified this matches your organization's data residency commitments and regulatory obligations?
DPA coverage	Does your existing SAP DPA cover this platform, or is a separate agreement required? Who negotiates and manages it?
Deletion fulfillment	When a customer exercises a GDPR or CCPA deletion right, can you guarantee complete deletion across SAP and this platform end-to-end?

Compliance and vendor risk

Certification basis	Are compliance certifications independently audited or self-attested? When were they last renewed?
Review overhead	What is the annual cost — in legal, security, and procurement time — to review and renew this vendor relationship?
Patch SLA	What is the vendor's SLA for critical security patch deployment? Does it align with your organization's vulnerability management standards?
Contract exit	If you terminate the relationship, what happens to your customer data? What are the portability guarantees and migration path?
Subprocessor disclosure	What third parties does this vendor share your customer data with? Is the subprocessor list disclosed and current? Is there a contractual notification requirement when the subprocessor list changes? This surfaces in every GDPR-serious organization and is rarely addressed at contract signature.



Audit Your Own Stack First

Apply this framework to your current platform first. The gaps it surfaces are the conversation to have — not a sales conversation about SAP Engagement Cloud, but a risk conversation about your existing architecture. That framing is more durable internally and doesn't require anyone to relitigate a purchasing decision.

08 Findings and Recommended Next Steps

What to do with this assessment internally.

What this assessment typically finds

For most enterprise SAP environments running a third-party marketing platform, this assessment surfaces the same pattern: an integration that was scoped and built as a project but is now owned as ongoing operations, PII flows that weren't fully mapped at procurement time, and a compliance review cycle that runs in parallel to SAP governance without anyone having calculated its cumulative annual cost.

None of these are crisis-level findings. But they're genuine architectural risks — the kind that don't create visible problems until something changes, and then create significant ones.

How to use this document internally

The most effective way to raise these findings internally is through the vendor consolidation framework in Section 07, applied to your current platform. That positions the conversation as a risk evaluation — which it is — rather than a platform pitch. It gives you something concrete to put in front of procurement, legal, and your CISO without requiring anyone to defend a past purchasing decision.

If the answers to the framework questions reveal gaps you weren't aware of, those gaps are the priority. The consolidation case for SAP Engagement Cloud follows from the gaps, not the other way around.

The architecture question

The right framing internally isn't "should we switch to SAP Engagement Cloud?" It's "what does our current customer engagement architecture actually look like, who owns the risk, and is that distribution of ownership intentional?" Most IT leaders find that asking that question surfaces decisions that were made by default rather than design — and that's the conversation worth having.

What SAP Engagement Cloud changes specifically

For organizations already running SAP CX products: native SAP CX suite integration; bidirectional contact and account sync with SAP Sales Cloud through SAP Integration Suite on BTP; authentication through SAP Cloud Identity Services with no additional identity infrastructure; customer data hosted within SAP-managed infrastructure under existing DPA; ISO/IEC 27001, GDPR, CCPA compliance absorbed into existing SAP governance cycle; a REST API with OAuth 2.0 and webhook architecture for custom scenarios where needed; and a 99.7% contractual SLA.

Next steps — on your terms

There are three ways to go deeper, in order of friction:

1 **Run the TCO Calculator**
Quantify what your current architecture is costing IT — integration maintenance hours, engineer cost, vendor review cycles. Enter your numbers and get back a specific figure you can use in an internal risk review or budget conversation, before you involve anyone from SAP. No form required to see your results. (sap.com/engagement-cloud/tco-calculator)

2 **Download the Architecture Brief**
A shorter technical reference covering integration architecture, data residency, identity, and compliance posture — formatted to share with your integration architect or CISO without requiring them to read the full assessment. (sap.com/engagement-cloud/architecture-brief)

3 **Request a technical conversation**
If you want a precise picture of what a consolidation or new deployment involves in your specific SAP environment — integration scope, identity configuration, data migration, compliance transition — your SAP account team can connect you with a solution architect. This is a scoping conversation, not a sales presentation.

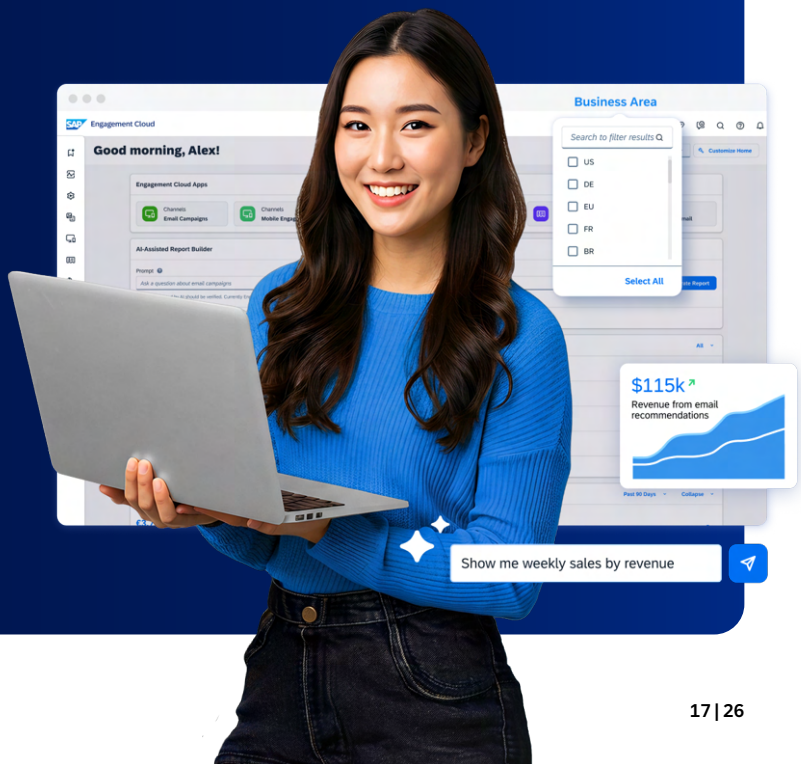
About SAP Engagement Cloud

SAP Engagement Cloud (formerly SAP Emarsys) enables teams and AI agents to power unique engagement by connecting real-time customer insights with the operational signals that run the business. As part of SAP's Customer Experience (CX) portfolio, Engagement Cloud enables personalized, AI-driven interactions across every channel—turning moments like orders, service events, and loyalty milestones into timely, relevant experiences that build trust, strengthen relationships, and drive growth.

It serves enterprise organizations across retail, consumer products, financial services, and B2B industries in more than 70 countries. Built on 25 years of engagement expertise, it enables marketing teams to activate customer data and build an infrastructure that IT teams already govern.

→ Developer documentation:
dev.emarsys.com

→ SAP Trust Center:
sap.com/trust-center



SAP Engagement Cloud helps organizations power unique engagement by connecting real-time customer insights with the operational signals that run the business. As part of the SAP Customer Experience (CX) portfolio, Engagement Cloud enables personalized, AI-driven interactions across every channel—turning moments like orders, service events, and loyalty milestones into timely, relevant experiences that build trust, strengthen relationships, and drive growth. For more information, visit: www.emarsys.com