Three deployment options for managing your cross-channel campaigns

Adobe

Executive summary

Marketers use campaign-management solutions to reach consumers across marketing channels with personalized, contextual experiences. To be effective, these solutions must overcome data-management, execution, security, and privacy challenges, among other things. Where you choose to deploy software and data affects your financial, technical, management, and regulatory costs, risks, and benefits of campaign-management solutions. The software and data deployment model you choose should align with your company's goals and resources.

This paper outlines the challenges of running personalized cross-channel campaigns and how they're affected by three deployment models for campaign-management solutions: at an on-premises data center, hosted in the cloud, or a hybrid model. A *chart* on page 11 compares these options and helps you choose the best model.

Cross-channel promise and challenges.

A central promise of data-driven marketing is *personalization*—reaching out to individuals based on who they are as well as where they're located or which device they're using. Consistent, personalized, contextual experiences are more engaging for consumers and more effective for marketers, but they can be difficult to execute.

State-of-the-art campaign-management solutions simplify and accelerate the planning, management, execution, and optimization of personalized cross-channel campaigns[1]—capabilities for which campaign managers acknowledge they need help:

- 66% of survey respondents said they don't view their marketing engagement strategies as customer-centric

- Only 21% said they use A/B or multivariate testing to determine the optimal campaign, content, or offer to deliver

- 80% can engage with customers in outbound channels, and 75% can engage with customers in inbound channels, but 69% struggle to combine these channels in an orchestrated, consistent fashion

Data management

Cross-channel personalization can be challenging for many reasons. First, data from multiple channels is *fragmented*—it can't be put to work until it's integrated into profiles that give marketers a single view of the customer. Legal, contractual, and other restrictions may also apply when integrating consumer data from different sources.

1. Assessing campaign management maturity: highlights from the 2014 Adobe Benchmark Survey. (San Jose, CA: Adobe Systems Incorporated, April 2014).
2. Preparing for Cross-Channel Success: Solving the Identity Puzzle (Chicago: Signal, March 2015).

Marketers report data fragmentation challenges

Marketers understand the difficulty of data management, as a 2015 survey[2] makes clear:

- **Collecting** cross-channel data was identified as a challenge by 55% of surveyed marketers.

- **Merging** the data into profiles caused difficulties for 57%.

- **Activating** matched profiles across the marketing ecosystem challenged 30%.

Execution

Even with customer profiles in hand, marketers still face operational challenges in executing cross-channel campaigns, including:

- *Speed*—especially when they involve multiple steps or contingencies, campaigns must execute in near real time to seem responsive
- *Complexity*—the ever-growing volume of data and number of online and offline, mobile, location-based, and social touchpoints increases execution time and expense
- *Context*—consumers resent out-of-context messages, but it's difficult to maintain context in complex or one-to-one campaigns
- *Fatigue*—consumers who receive too many campaign communications may develop message resistance and opt out
- *Return on investment*—marketing is still accountable for mounting effective campaigns, even when response rates fall due to outside or global factors

Campaigns that were rate-limited by the speed of physical mail or telephone call centers could still be managed by hand. But for today's pure digital or cross-channel campaigns, especially multi-stage campaigns with contingent contextual or remarketing steps, automation is a necessity.

Regulation

In pre-digital campaigns, multiple safeguards protected customer data. Database marketers could rely on their own expertise and experience, as well as follow codes of conduct published by professional organizations. The data itself came with protections—isolation within marketing for first-party lists, carefully defined agreements for second-party data-sharing partnerships, and detailed contracts for renting third-party lists. Finally, the relatively low volume and velocity of campaigns kept data from getting out of control too quickly.

Digital has changed all that. Digital convergence has pulled together marketing departments, eliminating the old specializations and separation of powers. Data from web behavior and connected objects, for example, are more difficult to curate and manage. Sometimes new touchpoints even create new data categories. Attractive opportunities to combine data sources raise important questions about permissions. And the scale and speed of digital campaigns threaten to overwhelm the old controls.

New systems have replaced legacy systems that limited data use and storage. Increased public awareness of digital databases, combined with high-profile breaches of retail customer databases and disclosure of

government surveillance programs have raised the regulatory profile of digital marketing. Digital campaigns must now comply with data-protection, privacy, opt-in, and "right-to-be-forgotten" requirements that vary across jurisdictions, and may even include limitations on data movement between jurisdictions.

In short, new technologies have extended the speed, scope, and effectiveness of marketing campaigns beyond the limits of what could be done before. But these same technologies have introduced new challenges of managing data, execution, and regulatory risk. How well do campaign-management solutions address these challenges?

Some of the challenges can be, and have been, addressed by new or modified features—encryption and anonymization protocols to protect private data, for example. Others, including performance and regulatory challenges, must be met by selecting the right deployment model. We'll look at the different ways campaign-management solutions can be implemented, and outline the advantages and drawbacks of each model.

Security and privacy protections for services hosted in the cloud

The highest priority of any cloud services provider is protecting the security and privacy of information their clients entrust to them. Adobe makes it a top priority to implement security and privacy controls beyond the scope—and often beyond the resources—of companies responsible to protect only their own data.

Sophisticated security management combines both top-down and bottom-up security and privacy activities, illustrated in Figure 1. Top-down activities establish, manage, and monitor processes during product development. Adobe identifies these processes as the Adobe Secure Product Lifecycle—hundreds of security activities spanning software development practices, processes, and tools, integrated across multiple stages of the product lifecycle.

Bottom-up security and privacy controls and processes are organized into compliance frameworks. Security certifications document compliance of an organization's facilities, computing infrastructure, operations, and software with the framework.

To learn more, see our *Adobe Security and Privacy Certifications* white paper. To discuss the specifics of controls and data protections, you can make arrangements with your Adobe representative.
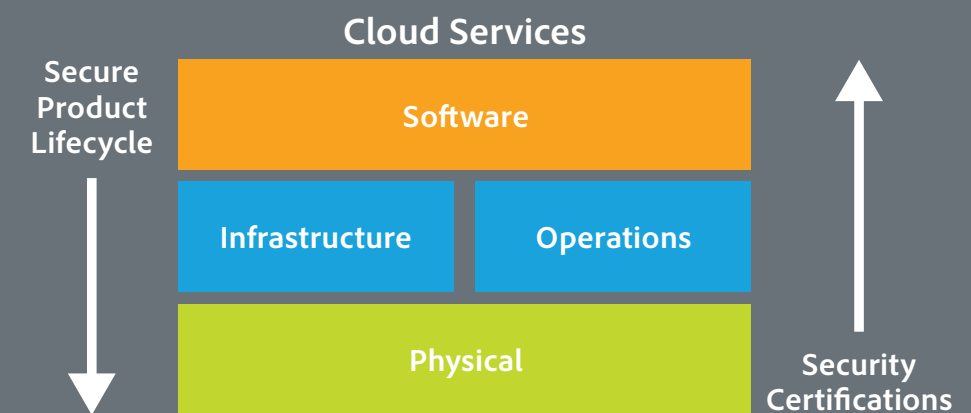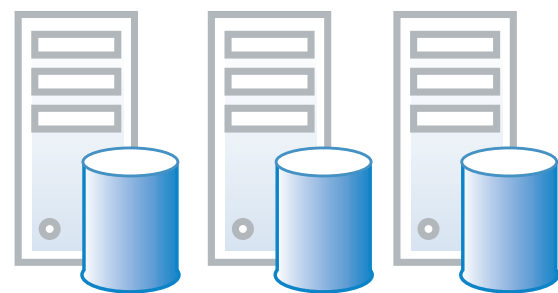

Figure 1: Security and privacy depend on both top-down and bottom-up activities.

On-premises model

For many years, implementing campaign-management solutions on a company's own hardware in its own data center was the only option available, and it continues to be the most popular option. The model maintains the traditional roles of marketing as client and IT as service provider.

Advantages of the on-premises model include:

- *Local control* over the application and all data, including integrations with Customer Relationship Management (CRM), financial, and other systems that may contain highly sensitive personal customer information

- *Simplified compliance* with data-protection and privacy requirements, especially when personal information can be kept at a data center in the same jurisdiction where it originates

- *Custom configuration* of hardware and software to meet unique security, performance, interface, or other requirements

- *Seamless integration* with other (homegrown) on-premises software solutions

Disadvantages of the on-premises model include all the reasons companies are moving development, campaign execution, and even mission-critical workloads to the cloud:

- *Capital expense*—infrastructure to run and integrate applications must be built, housed, powered, cooled, and connected

- *Operational expense*—recurring costs, including those for hiring, training, and retention of skilled personnel, are often much higher

- *Scalability*—IT must build infrastructure to avoid capacity caps, even when demand is seasonal or intermittent—often the case with campaigns

- *Time-to-market and agility*—when introducing or scaling services requires new infrastructure or integration, delays can be significant and expensive

- *Global availability and performance*—redundant, high-end hardware is expensive, and solutions not deployed globally will suffer from propagation delays

- *Security resources*—corporate IT departments will likely have less time, attention, and specialized staff available for data protection than specialist service providers

Most brands with established on-premises solutions, successful relationships between marketing and IT, and low-to-moderate regulatory risks will be conservative about moving from a deployment model that works well for them, especially after their initial capital costs have been fully absorbed. On-premises deployment is an especially attractive option for companies in regulated industries like healthcare or financial services, where documented control over customer, lead, patient, or partner data is required. Yet they may want to review their position before license renewals, major upgrades, and periodically as economies of scale continue to improve alternative deployment models, like those described in the following pages.

On-premises deployment is an especially attractive option for companies in regulated industries like healthcare or financial services.

Marketing cloud model

The cloud model offers campaign-management software as a service, often sharing a platform with content management, analytics, and other marketing solutions. The economics of the cloud invert most of the disadvantages of on-premises deployment:

- *Initial capital expense* is much lower, and most pricing follows a subscription model

- *Operational expense* is shared across many subscribers instead of concentrated in local IT, resulting in significant economies of scale

- *Scalability* is built into cloud models; demand is averaged across many clients, smoothing out the peaks

- *New capacity* is usually available on short notice, without waiting for local IT resources

- *High-performance infrastructure* is typical, with multiple data centers worldwide

- *First-rate security infrastructure*, backed by full-time teams of specialists, is the industry standard

In addition, the cloud model ensures that the application is as up-to-date as possible. That includes:

- *Application management,* including monitoring, an accelerated pace of update management, and performance optimization

- *Reliability, availability, and performance,* with resilient infrastructure, tested backup and recovery processes, and multiple disaster recovery (DR) sites

- *Integration* among other marketing solutions, with common templates, consistent user interfaces, shared platform services, and accelerated data flows

Brands new to campaign management, struggling with poorly integrated point solutions or experiencing low project throughput using internal resources are the most promising candidates for the marketing cloud deployment model. The low costs and risks of trying out a cloud solution make it an attractive way to test the software, even for brands that plan to use an on-premises model, or a hybrid between on-premises and the cloud.

Hybrid model

The hybrid deployment model combines the benefits of on-premises and cloud deployments to address cost, scalability, performance, risk, and compliance issues. This option separates the application from execution management and database components; and deploys them separately:

- *Deployment in your data center* allows responsive segmentation, workflow, visualization, and execution triggering, as well as secure management of all letter, image, and template content
- *Message execution,* including bounce, tracking, and deliverability management, is delivered as a cloud service from secure, high-performance data centers
- *Data* remains in the client's own data center until the moment of campaign execution

The hybrid model reduces costs to launch or scale up campaigns, because high-performance execution infrastructure is maintained and professionally managed offsite. Clients maintain full management control over their campaign and databases, outsourcing only execution.

Data remains in the client's own data center until the moment of campaign execution.

Choose the best deployment model for your business

	EVALUATION METRIC	ON-PREMISES	MARKETING CLOUD	HYBRID
Financial	Capital expense	Expenses to build and maintain solution, database, and execution infrastructure	No new infrastructure; low initial capital expenses	Expenses to build and maintain solution and database infrastructure only
	Operational expense	Unlimited usage of IT resources; client bears operations, maintenance, personnel, and bandwidth costs	Subscription price for service; email sending included in hosting fee	Operations and maintenance costs on solution and database infrastructure only
	Scalability	Must build or reserve capacity to handle peak loads, or tolerate substantial delays	Rapid, virtual scaling; provider manages bandwidth, IP, load balancing	Rapid, virtually scale-up; provider manages bandwidth, IP, load balancing
Performance	Time-to-market, agility	At launch, time to build and staff all infrastructure; slow to scale up or down	Rapid start; low cost and risk of trial period; scales quickly up or down	At launch, time to build and staff solution and database infrastructure; scales quickly
	Global availability and performance	Limited by number and distribution of deployments and data centers; expensive	Distributed data-collection and computing centers—no impact on local network resources; multiple DR sites	Distributed data-collection and computing centers; multiple DR sites
Management	Security resources	Time and attention spread across many applications and commitments	Well-staffed, trained, and equipped; mature governance and compliance processes	Well-staffed, trained, and equipped; mature governance and compliance processes; security resources limited to execution
	Application management	Local monitoring responsibilities; slow pace of upgrades and updates	Continuous monitoring, upgrades and updates between release dates	Application is on premises with local monitoring; slow pace of upgrades and updates
	Solution integration	Tight integration with other information systems is possible; integration is responsibility of local IT staff	Integrated solutions delivered on a platform of common services	Responsibility of IT staff to integrate solutions
Privacy/security	Data privacy control and compliance	Data reside only on-premises; encryption local responsibility; simplified compliance reporting	Data are handled externally using encrypted transmission and storage; compliance reporting is shared	Data reside on-premises, are transmitted encrypted and temporarily stored externally; shared compliance reporting
	Access control	Local control and responsibility by data center staff; insider attack is possible	Mature, documented physical security, personnel screening, authentication, and other controls	Local responsibility at brand data center; insider attack is possible

Adobe Campaign provides best-in-class campaign, offer, and personalization management capabilities for sophisticated automation and execution of marketing programs across all channels—digital and traditional. Adobe Campaign addresses a key challenge for marketers: how to build and extend relationships with their customer base to drive top-line revenue growth and ROI. Adobe Campaign is used by approximately 650 of the world's leading brands. Allowing every company to select the best fit based on their marketing strategy, IT ecosystem, and business and legal requirements, Adobe Campaign is the only solution to offer three deployment models—on-premises, cloud and hybrid. Marketers finally have a complete, integrated yet flexible solution for their marketing efforts.

https://www.adobe.com/marketing-cloud/campaign-management.html

Adobe Marketing Cloud empowers companies to use data-driven marketing to reach and engage customers and prospects with highly personalized marketing content across devices and digital touch points. Eight tightly integrated solutions offer marketers a complete set of marketing technologies that focus on analytics, web and app experience management, testing and targeting, advertising, audience management, video, social engagement and campaign orchestration. The tie-in with Adobe Creative Cloud makes it easy to quickly activate creative assets across all marketing channels. Thousands of brands worldwide, including two thirds of Fortune 50 companies, rely on Adobe Marketing Cloud with over 41 trillion transactions a year.

https://www.adobe.com/marketing-cloud.html