Adobe Experience Cloud

Adobe

WHITEPAPER

Adobe® Marketo Engage Security Overview

Table of Contents

Adobe Security 2

About Marketo Engage 2

Marketo Engage Solution Architecture 2

Marketo Engage Data Flow Narrative 4

Marketo Engage Security Architecture 6

Marketo Engage User Authentication 6

Additional Security Customizations 7

Marketo Engage Hosting and Security 8

Adobe Security Program Overview 9

Conclusion 14

Adobe Security

At Adobe, we know the security of your digital experience is important. Security practices are deeply ingrained into our internal software development, operations processes, and tools. These practices are strictly followed by our cross-functional teams to help prevent, detect, and respond to incidents in an expedient manner. We collaborate with partners, leading researchers, security research institutions, and other industry organizations to keep up to date with the latest threats and vulnerabilities. We regularly incorporate advanced security techniques into the products and services we offer.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to secure Marketo Engage and its associated data.

About Marketo Engage

Marketo Engage brings together marketing and sales in a single solution designed to orchestrate personalized experiences, optimize content, and measure business impact across every channel, from consideration to conversion and beyond.

Marketo Engage Solution Architecture

The Marketo Engage solution includes the following components:

- **Marketo Lead Management** (MLM) — The core of the Marketo Engage application, MLM is where customers launch marketing programs, create campaigns to nurture leads, design landing page and email assets, and report on performance metrics.
- **Revenue Cycle Analytics** (RCA) — Enables users to report on the performance of their marketing efforts, including opportunity attribution, email performance, and lead generation.
- **Web Activity Tracking** — A JavaScript, called Munchkin.js, that customers place on their websites to collect information on page visits and clicks for use in Marketo Engage lead nurturing.
- **Marketo User Interface** — Customers interact with the Marketo Engage solution using the Marketo UI. Administrators use the same UI to authorize Marketo Engage and integration users (see next bullet for more information).
- **APIs** — Enable third-party developers to integrate their solutions with Marketo Engage using REST or SOAP API calls.
- **LaunchPoint Integrations** — Marketo-built and -maintained integrations with webinar providers and ad platforms.

- **Native CRM Integrations** — Marketo-built and -maintained connectors to the Salesforce.com and Microsoft Dynamics CRM platforms.

- **Marketo Sales Insight** (MSI) — App packages that customers can install in their Salesforce or Microsoft Dynamics environments, which allow CRM users to view Marketo Engage lead data and trigger Marketo Engage emails and marketing campaigns.

- **Add-on Modules** — Customers can extend their Marketo Engage solution with one or more of the following Marketo modules, available at additional cost:
  - Sales Connect – Engage sales leads via multiple channels throughout the sales cycle
  - Target Account Management – Target, score, and engage with key accounts
  - Web Personalization –Target key audiences and serve them personalized content
  - Predictive Content – Engage web visitors and email recipients with the most relevant content, using suggestions powered by machine learning and predictive analytics
  - SEO – Track website performance in search engines and provide guidance in improving rankings
  - Marketo Mobile Engagement – Integrate with smart phone applications to track engagement, target audiences, and push notifications

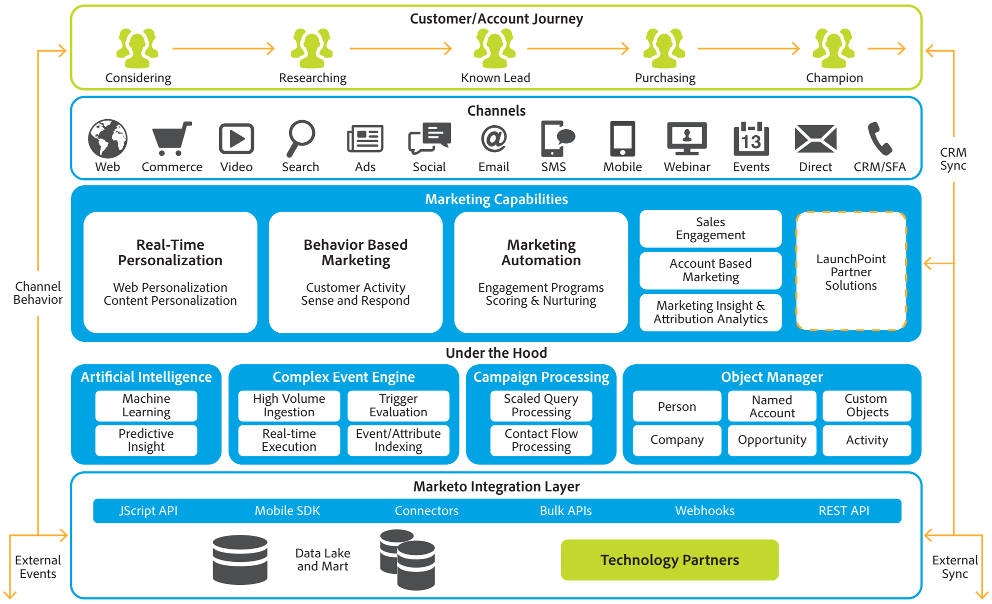


Figure 1: Marketo Engage solution architecture

Marketo Engage Data Flow Narrative

The following bullets describe how data flows into and out of a Marketo Engage implementation:

- The customer determines where to deploy landing pages, forms and media, which are supported by the Marketo Engage munchkin.js cookie and other tracking technologies. These forms and tracking technologies collect data from visitors to the customer's website and landing pages, which is then transmitted to and stored in the customer's Marketo database at the applicable data center. Data collected from visitors can include device IP address, geolocation data inferred from IP lookups, and personal data collected by forms.
- Lead data can enter Marketo Engage from external sources managed by the customer. These sources include:
  - List imports – Users can import .csv files of lead data mapped to Marketo Engage lead fields
  - REST/SOAP APIs – External integrations may push data into Marketo Engage using publicly available APIs or webhooks
  - LaunchPoint integrations – Third-party integrations with webinar providers, ad platforms, social media platforms, and other services approved (but not operated) by Marketo, may synchronize lead and device data between the third-party service and Marketo Engage
  - Manual input – Users may manually create and update lead data in the application

- Marketo Engage supports automatic two-way synchronization with Salesforce.com and Microsoft Dynamics CRM platforms. Enabled subscriptions sync lead, contact, account, and other data using internal APIs encrypted via HTTPS.
- Marketo Engage interprets data, such as demographical and behavioral information, stored in the database to nurture leads throughout the marketing and sales lifecycle, including to target audiences for marketing campaigns.
- If a user initiates an email from Marketo Engage to a natural person, lead data can be used to personalize the email content. This data can consist of Personally Identifiable Information (PII) collected by the customer from the person or data maintained by the customer, such as an account number, to facilitate the relationship. In order to enable metrics reporting, such as email open rates as well as IP address, email client, and other device information, data may flow from the recipient of an email back to the customer's Marketo database by means of a tracking pixel embedded in the email.
- Web content, including landing pages, forms, and posts on social media can be dynamically personalized to incorporate lead data in the design, e.g., welcoming a visitor by their first name.

- Marketo Engage users with sufficient permissions can initiate exports of all lead data from the UI for use in external applications.
- If Marketo Sales Insight is installed in an environment integrated with Salesforce.com or Microsoft Dynamics, customer data can flow between the platforms, allowing CRM users to view Marketo Engage-hosted lead data and to trigger marketing campaigns. This data flow utilizes the application's internal APIs and is encrypted via HTTPS.
- Certain processing operations, such as the Predictive Content and Marketo Mobile Engagement offerings, rely upon data service providers, known as sub-processors, for specific and limited feature capabilities. When a sub-processor is used, customer data flows from the Marketo database to the sub-processor and back again after processing.
- If the customer chooses to extend their deployment with one of the Marketo add-on packages, such as Target Account Management or Advanced BI Analytics, lead data flows between them.
- If the customer chooses to deploy a third-party solution that is already integrated with Marketo or uses Marketo's API to integrate with a new third-party or proprietary solution, the data that flows between the solutions depends on the customer's specific implementation.

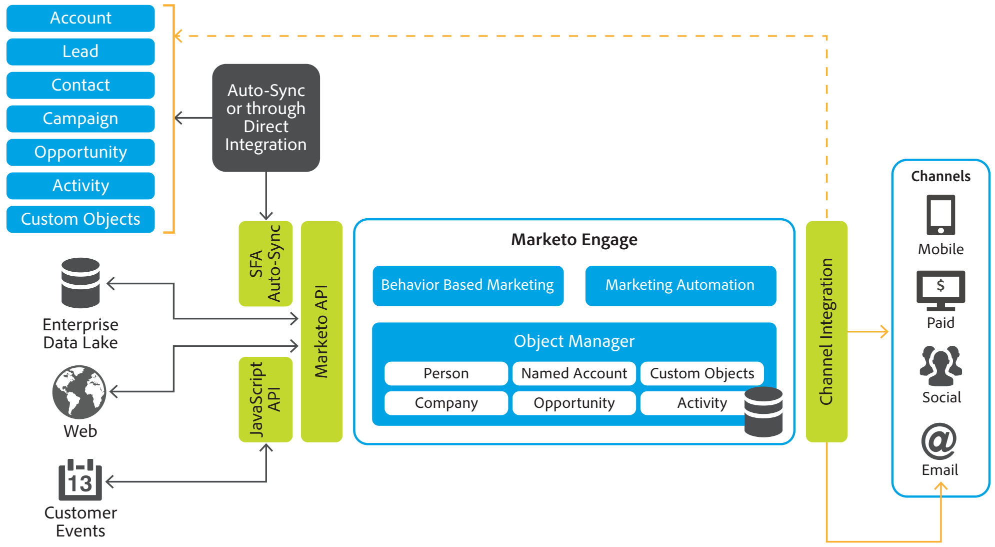


Figure 2: Marketo Engage Data Flow

All connections between Marketo Engage components as well as connections to external components are conducted over secure, encrypted connections.

[1] The sub-processors applicable to a customer's use of Marketo depend upon which services the customer selects for their package. A list of all sub-processors is publicly available at https://documents.marketo.com/legal/sub-processor-list/.

Marketo Engage Security Architecture

The following network diagram depicts the Marketo Engage security architecture:

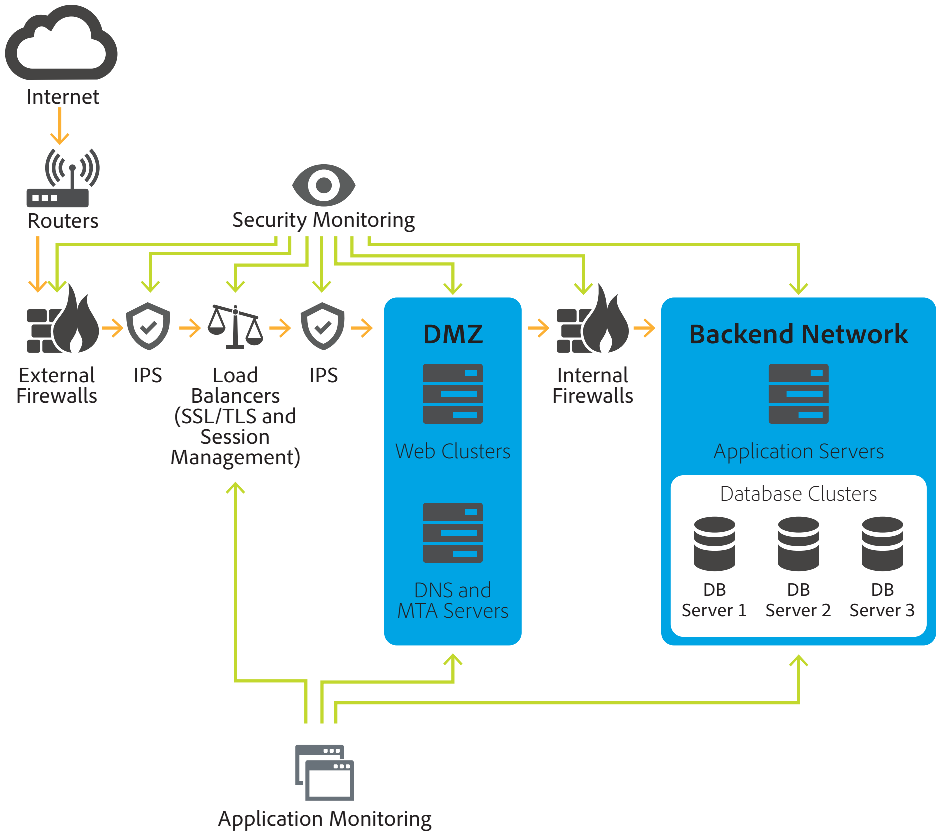


Figure 3: Marketo Engage Network Security Architecture

Data encryption

Marketo Engage uses HTTPS TLS v1.2 to protect data in transit. For an additional fee, customers may purchase the ability to encrypt data at rest with AES 256-bit encryption.

Marketo Engage User Authentication

Marketo applications are accessible via any browser-enabled client, and support IP range restriction, including allow lists and deny lists. User login and data actions are tracked in audit logs. Session timeouts automatically log an idle user out of the applications. SaaS instance administrators can set password strength parameters that enforce length, case, mixed case, number, special characters, and expiration.

To prevent password-guessing (brute force) attacks, account access is locked automatically after five (5) unsuccessful attempts to guess a password.

Marketo also supports customers' enterprise Single Sign On (SSO) using SAML v2.

Additional Security Customizations

Marketo Engage enables the following additional controls:[2]

- **Role-based access** — Marketo users are granted role-based access by the administrators. Access permissions are based on assigned user roles, which specify security rights for normal users, power users, and system administrators. In addition to predefined roles, administrators can create additional roles, with more than 100 available access permissions.
- **Access segmentation** (Workspaces) — To restrict data access based on data values, Marketo administrators can implement workspaces. For example, users can be given access only to accounts or regions assigned to them.
- **Device authorization** —Customer logins to the Marketo solution from unrecognized network locations trigger a device authorization check in the form of an additional token verification, in which a token is sent to the account's registered e-mail address for validation.
- **IP restrictions** — Marketo supports customer-controlled allow listing or deny listing of specified IP addresses and networks.
- **Configurable password parameters** — Administrators can configure complexity, length, limited attempts and expiration of user passwords.
- **Antivirus** — Antivirus checks and blocking of potentially unsafe files are performed on all uploaded data.
- **Account creation notification** — Administrators are notified when a new admin account is created.
- **High security mode by default** — When a new Marketo subscription is activated, security parameters are set to the most stringent security and can be adjusted as needed by the subscription administrator.
- **Session timeout** — Marketo administrators can configure Inactive sessions timeout.

[2] All customizations except antivirus are controlled by the Marketo Engage administrator. Antivirus is enabled on all subscriptions and cannot be disabled.

Marketo Engage Hosting and Security

The Marketo Engage service infrastructure resides in enterprise-class data centers or co-locations from top-tier cloud hosting providers in San Jose, CA and Ashburn, VA in the United States; London, England; and Sydney, Australia, as well as in an Adobe-managed data center in Amsterdam, The Netherlands.

All data centers provide the full range of hosting facility features, such as fully redundant power and environmental systems as well as industry-leading and third-party audited levels of security.

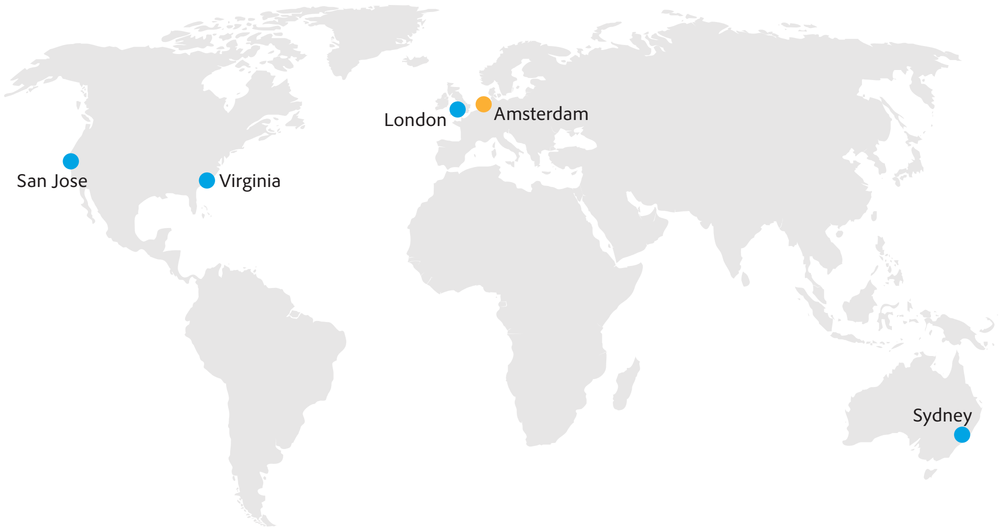


Figure 4: Marketo Data Center Locations

For more information on Amazon Web Services security, please see https://aws.amazon.com/security

For more information on Microsoft Azure security, please see https://azure.microsoft.com/en-us/services/security-center/

For more information on Google Cloud security, please see https://cloud.google.com/security

Adobe Security Program Overview

The integrated security program at Adobe is composed of five (5) centers of excellence, each of which constantly iterates and advances the ways we detect and prevent risk by leveraging new and emerging technologies, such as automation, AI, and machine learning.

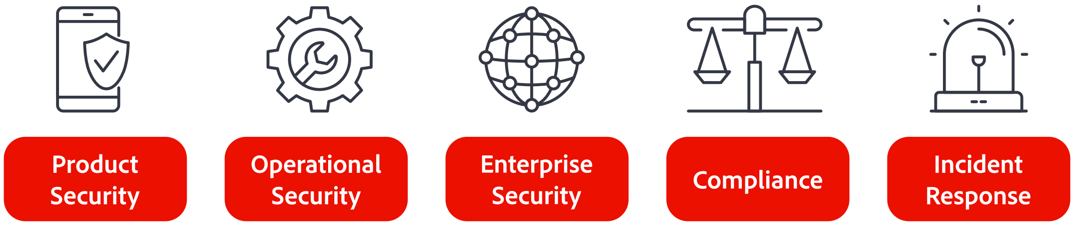


Figure 5: Five Security Centers of Excellence

The centers of excellence in the Adobe security program include:

- **Application Security** — Focuses on the security of our product code, conducts threat research, and implements bug bounty.
- **Operational Security** — Helps monitor and secure our systems, networks, and production cloud systems.
- **Enterprise Security** — Concentrates on secure access to and authentication for the Adobe corporate environment.
- **Compliance** — Oversees our security governance model, audit and compliance programs, and risk analysis; and
- **Incident Response** — Includes our 24x7 security operations center and threat responders.

Illustrative of our commitment to the security of our products and services, the centers of excellence report to the office of the Chief Security Officer (CSO), who coordinates all current security efforts and develops the vision for the future evolution of security at Adobe.

The Adobe Security Organization

Based on a platform of transparent, accountable, and informed decision-making, the Adobe security organization brings together the full range of security services under a single governance model. At a senior level, the CSO closely collaborates with the Chief Information Officer (CIO) and Chief Privacy Officer (CPO) to help ensure alignment on security strategy and operations.

In addition to the centers of excellence described above, Adobe embeds team members from legal, privacy, marketing, and PR in the security organization to help drive transparency and accountability in all security-related decisions.

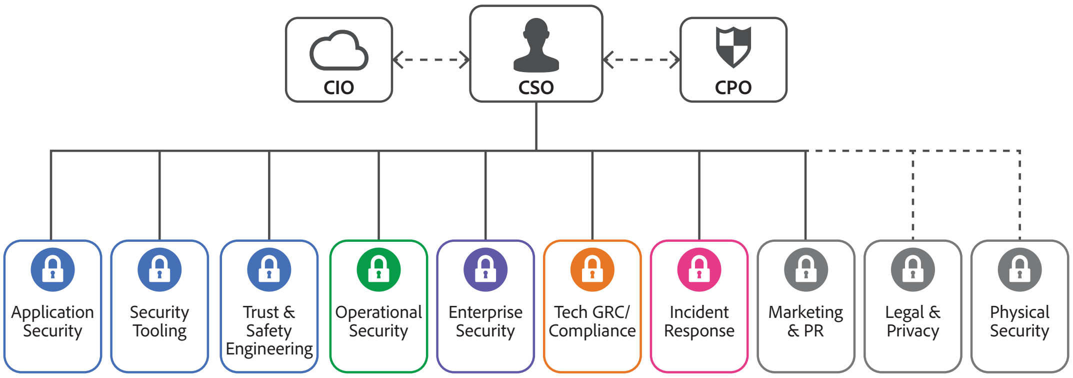
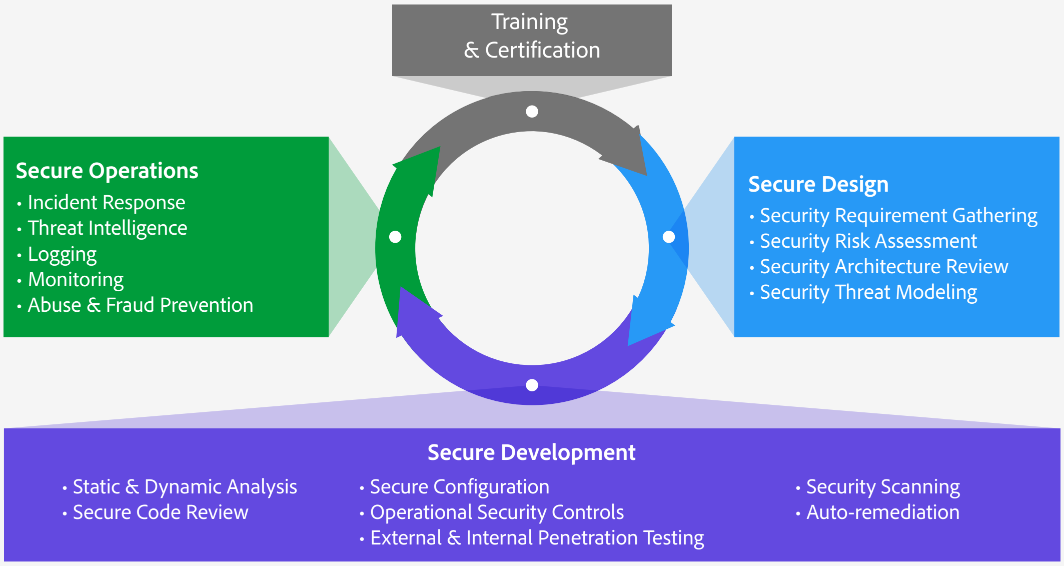


Figure 6: The Adobe Security Organization

As part of our company-wide culture of security, Adobe requires that every employee completes our security awareness and education training, which requires completion and re-certification on an annual basis, helping ensure that every employee contributes to protecting Adobe corporate assets as well as customer and employee data. On hire, our technical employees, including engineering and technical operations teams, are auto-enrolled in an in-depth 'martial arts'-styled training program, which is tailored to their specific roles. For more information on our culture of security and our training programs, please see the Adobe Security Culture white paper.

The Adobe Secure Product Lifecycle

Integrated into several stages of the product lifecycle—from design and development to quality assurance, testing, and deployment— the Adobe Secure Product Lifecycle (SPLC) is the foundation of all security at Adobe. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC defines clear, repeatable processes to help our development teams build security into our products and services and continuously evolves to incorporate the latest industry best practices.



Training
& Certification

Secure Operations
- Incident Response
- Threat Intelligence
- Logging
- Monitoring
- Abuse & Fraud Prevention

Secure Design
- Security Requirement Gathering
- Security Risk Assessment
- Security Architecture Review
- Security Threat Modeling

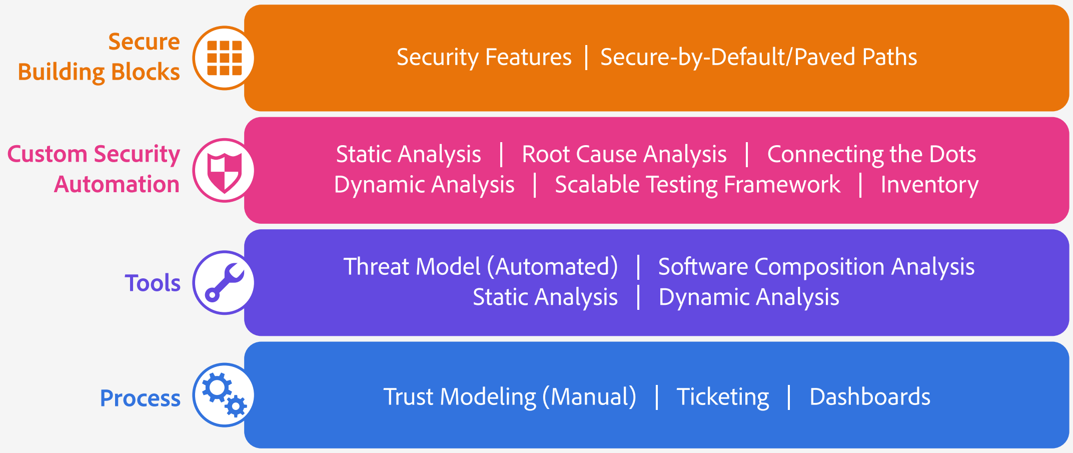
Secure Development
- Static & Dynamic Analysis
- Secure Code Review
- Secure Configuration
- Operational Security Controls
- External & Internal Penetration Testing
- Security Scanning
- Auto-remediation

Figure 7: The Adobe Secure Product Lifecycle

Adobe maintains a published Secure Product Lifecycle Standard that is available for review upon request. More information about the components of the Adobe SPLC can be found in the Adobe Application Security Overview.

Adobe Application Security

At Adobe, building applications in a "secure by default" manner begins with the Adobe Application Security Stack. Combining clear, repeatable processes based on established research and experience with automation that helps ensure consistent application of security controls, the Adobe Application Security Stack helps improve developer efficiency and minimize the risk of security mistakes. Using tested and pre-approved secure coding blocks that eliminate the need to code commonly used patterns and blocks from scratch, developers can focus on their area of expertise while knowing their code is secure. Together with testing, specialized tooling, and monitoring, the Adobe Application Security Stack helps software developers to create secure code by default.



Secure Building Blocks: Security Features | Secure-by-Default/Paved Paths

Custom Security Automation: Static Analysis | Root Cause Analysis | Connecting the Dots
Dynamic Analysis | Scalable Testing Framework | Inventory

Tools: Threat Model (Automated) | Software Composition Analysis
Static Analysis | Dynamic Analysis

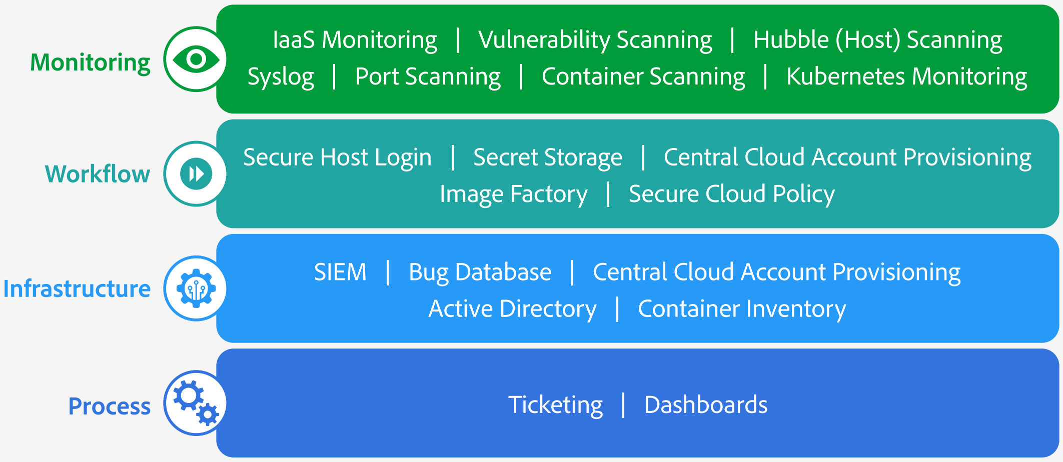
Process: Trust Modeling (Manual) | Ticketing | Dashboards

Figure 8: The Adobe Application Security Stack

Adobe also maintains several published standards covering application security, including those for work specific to our use of Amazon Web Services (AWS) and Microsoft Azure public cloud infrastructure. These standards are available for view upon request. For more information on Adobe application security, please see the Adobe Application Security Overview.

Adobe Operational Security

To help ensure that all Adobe products and services are designed from inception with security best practices in mind, the operational security team created the Adobe Operational Security Stack (OSS). The OSS is a consolidated set of tools that help product developers and engineers improve their security posture and reduce risk to both Adobe and our customers while also helping drive Adobe-wide adherence to compliance, privacy, and other governance frameworks.



Monitoring
IaaS Monitoring | Vulnerability Scanning | Hubble (Host) Scanning
Syslog | Port Scanning | Container Scanning | Kubernetes Monitoring

Workflow
Secure Host Login | Secret Storage | Central Cloud Account Provisioning
Image Factory | Secure Cloud Policy

Infrastructure
SIEM | Bug Database | Central Cloud Account Provisioning
Active Directory | Container Inventory

Process
Ticketing | Dashboards

Figure 9: The Adobe Operational Security Stack

Adobe maintains several published standards covering our ongoing cloud operations that are available for view upon request. For a detailed description of the Adobe OSS and the specific tools used throughout Adobe, please see the Adobe Operational Security Overview.

Adobe Enterprise Security

In addition to securing our products and services as well as our cloud hosting operations, Adobe also employs a variety of internal security controls to help ensure the security of our internal networks and systems, physical corporate locations, employees, and our customers' data.

For more information on our enterprise security controls and standards we have developed for these controls, please see the Adobe Enterprise Security Overview.

Adobe Compliance

All Adobe products and services adhere to the Adobe Common Controls Framework (CCF), a set of security activities and compliance controls that are implemented within our product operations teams as well as in various parts of our infrastructure and application teams. As much as possible, Adobe leverages leading-edge automation processes to alert teams to possible non-compliance situations and help ensure swift mitigation and realignment.

Adobe products and services either meet applicable legal standards or can be used in a way that enables customers to help meet their legal obligations related to the use of service providers. Customers maintain control over their documents, data, and workflows, and can choose how to best comply with local or regional regulations, such as the General Data Protection Regulation (GDPR) in the EU.

Adobe also maintains a compliance training and related standards that are available for review upon request. For more information on the Adobe CCF and key certifications, please see the Adobe Compliance, Certifications, and Standards List.

Incident Response

Adobe strives to ensure that its risk and vulnerability management, incident response, mitigation, and resolution processes are nimble and accurate. We continuously monitor the threat landscape, share knowledge with security experts around the world, swiftly resolve incidents when they occur, and feed this information back to our development teams to help achieve the highest levels of security for all Adobe products and services. We also maintain internal standards for incident response and vulnerability management that are available for view upon request. For more detail on Adobe's incident response and notification process, please see the Adobe Incident Response Overview.

Business Continuity and Disaster Recovery

The Adobe Business Continuity and Disaster Recovery (BCDR) Program is composed of the Adobe Corporate Business Continuity Plan (BCP) and product-specific Disaster Recovery (DR) Plans, both of which help ensure the continued availability and delivery of Adobe products and services. Our ISO 22301-certified BCDR Program enhances our ability to respond to, mitigate, and recover from the impacts of unexpected disruptions. More information on the Adobe BCDR Program can be found here.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Marketo Engage and your confidential data. At Adobe, we take the security of your digital experience very seriously and we continuously monitor the evolving threat landscape to try to stay ahead of malicious activities and help ensure the security of our customers' data.

More information on Adobe security can be found on the Adobe Trust Center.

Adobe