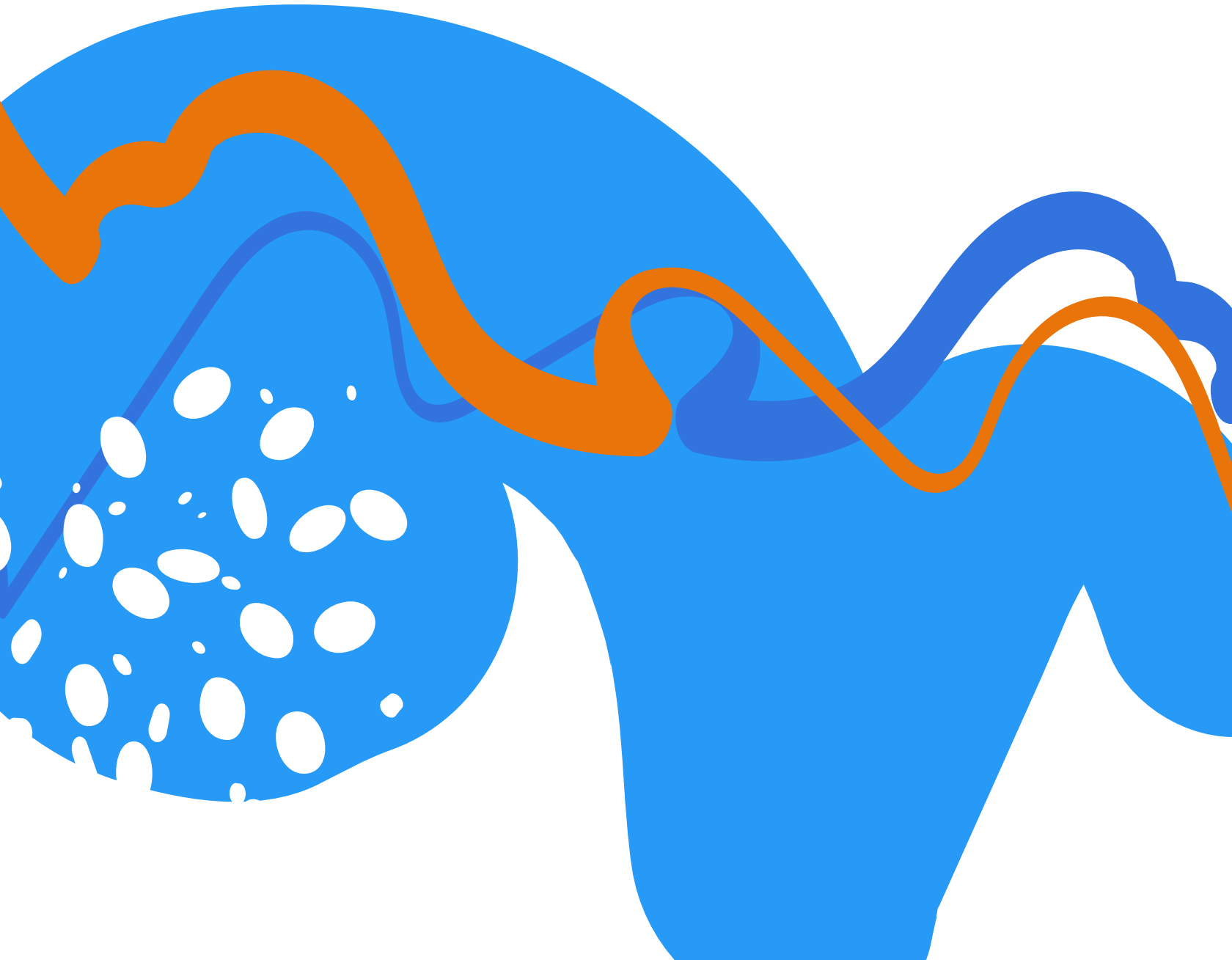
WHITE PAPER

# Adobe® Application Security Overview



# Table of Contents


**Introduction** 3

**The Adobe Application Security Strategy** 3

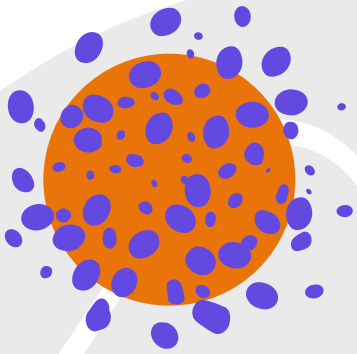
**The Adobe Secure Product Lifecycle** 3

**The Adobe Application Security Stack** 5

- Secure Blocks 5
- Security Automation 6
- Process 7

**Looking Ahead: The Service Lifecycle (SLC)** 8

**Conclusion** 9

# Introduction

At Adobe, secure application development is core to what we do, which is why we've made significant investments in security research and technology that comprise our Application Security team. Focused on keeping up with the pace of innovation while helping ensure Adobe products and services include the most effective security measures, the Application Security team helps our product and service teams across the company build applications in a "secure-by-default" manner. The team relies on a variety of automation approaches to gather data and help make risk-based decisions in order to improve the company's overall security posture.

This white paper describes the Adobe application security strategy, which focuses on introducing security controls early in the development cycle to help scale, reduce overall costs, and minimize the chances of actual security risks, all of which reinforces our commitment to modern security practices to protect Adobe and our customers' data and workflows.

# The Adobe Application Security Strategy

Our application security strategy focuses on solving security issues at the root cause rather than treating the symptoms. At Adobe, we do this by "shifting left" and introducing security earlier in the development lifecycle than common practice. By introducing security controls and mechanisms in the requirements, architecture, design, and coding phases of development, we can help bake in security controls and reduce the high cost of changes introduced later in the lifecycle, during testing and production. This approach also minimizes the chance of actual security risks, which translates to greater security for our customers.

# 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 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. SPLC controls include service roadmaps, security tools, and testing methods that guide the security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical application security flaws and CWE/SANS Top 25 most dangerous software errors.

Adobe security researchers provide specific SPLC guidance for each key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

The Adobe SPLC is organized into four key areas reflecting the full design, development, deployment, and ongoing operational lifecycle of Adobe products and services.

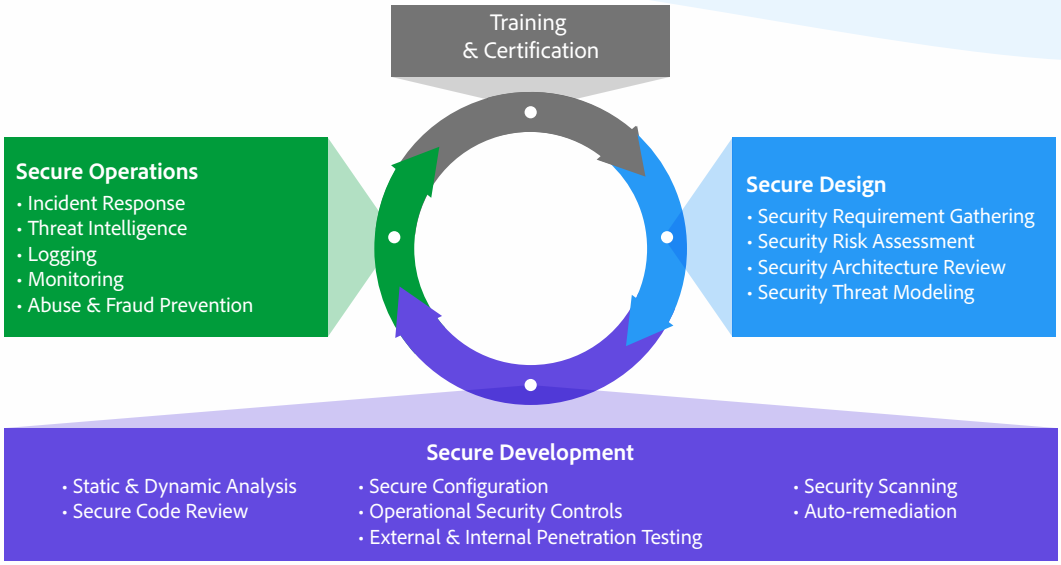



Figure 1: The Adobe Secure Product Lifecycle (SPLC)

The Adobe SPLC is implemented across the company and enforced by security researchers on the Adobe Application Security team, which advises our product and services teams on best practices for security controls and validates the security controls through the use of automation.

For more information about the Adobe SPLC and the Adobe Security Team, please see the Product Security section of the Adobe Trust Center.

# The Adobe Application Security Stack

Building secure-by-default applications at Adobe begins with the Application Security (AppSec) Stack, which includes secure building blocks, secure workflows, and a range of standardized, security-first tools that have been tested and approved by the Adobe Application Security team.

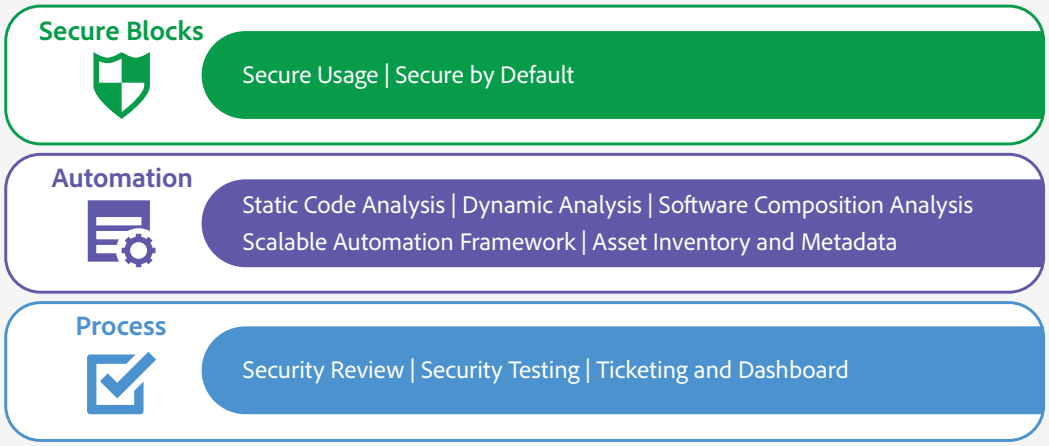



Figure 2: The Adobe Application Security Stack

Each of the three (3) layers in the Adobe AppSec Stack includes a range of tools and services that can be leveraged by any Adobe product team in their development process to help ensure security is built in every Adobe application from the ground up and reinforce our focus on modern security practices to protect customer data and workflows.

## Secure Blocks

With pre-approved building blocks, called Secure Blocks, Adobe developers gain a well-paved path that provides secure-by-default guardrails for application development. These blocks include verified and approved identity services, API gateways, messaging systems, SDKs, and frameworks that enable the rapid and secure development of Adobe products and services.

Secure Blocks not only allow for easy scaling, but they also help verify the correct usage of security features and configurations. Based on two main principles—detection and prevention—Secure Blocks include a set of continuous detection solutions to identify insecure usage along with preventive controls that help Adobe developers achieve a secure-by-default posture for their applications.

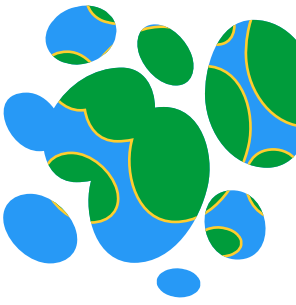
Secure Blocks help ensure the following:

- **Secure usage** — We use automation to identify security misconfigurations that can occur while using common platforms and building blocks within Adobe products and services. By continuously analyzing a vast set of configuration data, logs, and source code, we can quickly discover any deviations and alert the engineering team.
- **Secure by default** — Adobe continues to invest in security controls that follow secure-by-default principles—such as least privilege, default deny, and built-in authentication —in order to protect customer data and workflows. These investments enable our product teams to focus on their product expertise rather than on securing the workflow, making it easier to protect large numbers of workflows within the ecosystem.

## Security Automation

At Adobe, automation enables product security to scale across the company and to provide continuous security coverage to keep up with the rapid pace of innovation. Our static and dynamic analysis initiatives, which target software code, collections of configuration data, request/response traffic, and application logs, help Adobe to secure the entire software development lifecycle.

- **Static code analysis** — Our automated code analysis solution leverages both open source and commercial tools to scan code repositories at Adobe. We also continually add to and improve a variety of code analysis tools, which help to ensure the overall security of our code.
- **Dynamic analysis** — Similar to our approach to static code analysis, Adobe uses custom-built and commercial tools to identify security vulnerabilities at run time.
- **Software composition analysis** — We closely monitor the usage of third-party components in our products and services and regularly review the security posture of these components using both in-house and commercial solutions. When we find a vulnerable or end-of-life component, we alert the developers for timely mitigation.
- **Scalable automation framework (SAF)** — An internally developed tool for automating security checks across Adobe web properties in a scalable and extendable manner, SAF is built on a modular architecture that allows each component to be changed independently of each other and enables the recompilation of the entire tool set in a matter of minutes.
- **Asset inventory and metadata** — A rich set of metadata for the entire company helps our Application Security team gain deeper insights into Adobe applications and services. We use this information to power our automation, perform company-wide searches for potential holes, and generate security reporting.



# Process

Our in-house security expertise and processes form the foundation for security initiatives at Adobe. We continually invest in training both our security team members and Security Champions on emerging technologies and approaches, including AI and ML, with the goal of evolving our process for securing products. Ticketing, dashboarding, and effective risk mitigation through threat modeling is the fabric that binds security initiatives into an effective pipeline.

## Security Reviews

To provide security assurance across Adobe products and services, we have a stringent security review process, which uses a risk-based approach to prioritize areas of focus and identify security activities, including:

- **Threat modeling** — Performing a threat model during the design phase helps identify security flaws early in the development lifecycle and create a strong security foundation for each Adobe product and service. We conduct threat modeling to identify areas in which architectural changes may be required in order to avoid known threats. Using automation in the threat modeling process helps us scale effectively, automatically generating security requirements and making the review process more efficient. As an intelligent feedback loop, these threat models also help in performing targeted code review and security testing along with identifying high-impact areas for automation and secure-by-default application development.
- **Data Classification** — The data classification process validates that teams adhere to Adobe data classification standards, which are designed to manage information handling risk across the company.
- **Targeted code review** — For specific sections of code that deal with sensitive data or for components that are reused by multiple services, our expert security researchers perform manual code reviews to make sure that the code adheres to security best practices.
- **Targeted security testing** — Adobe security researchers spend dedicated time performing security testing of products and services based on multiple factors, including the type of data being transferred as well as emerging threats and attack patterns.

## Security Testing

In addition to regular security reviews, Adobe conducts penetration testing of our products and services that help strengthen areas of weakness and our bug bounty program engages our user community in detecting and reporting issues. Our security testing activities include:

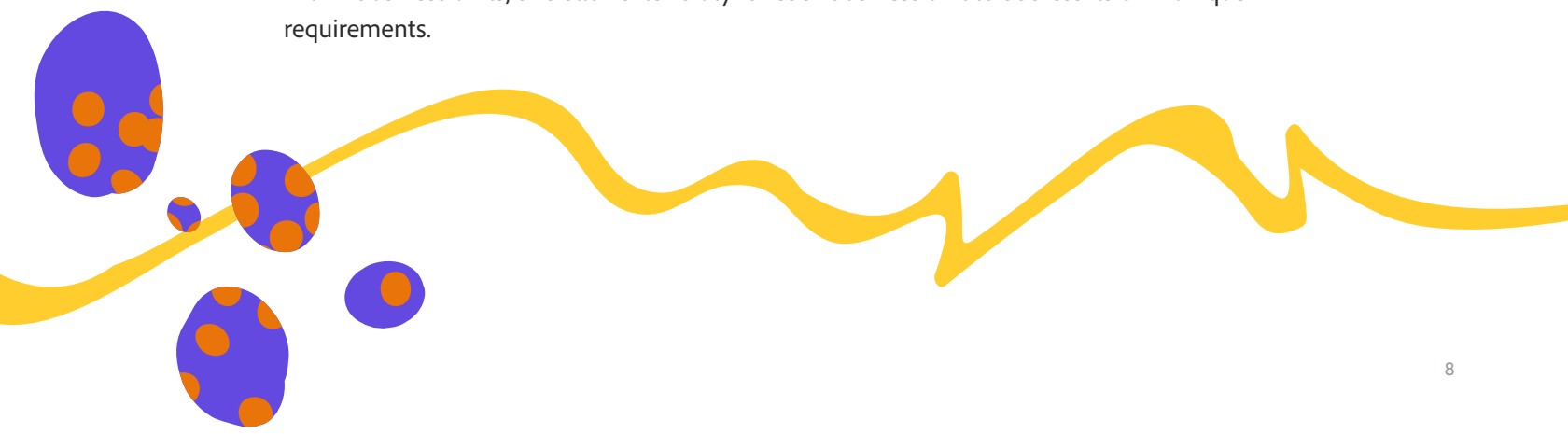
- **Internal Penetration Testing** — Adobe internal security teams perform code-assisted penetration testing using a combination of automated and manual techniques that target areas of weakness highlighted during the security review.
- **External Penetration Testing** — We engage with leading third-party security firms to perform penetration testing that can uncover potential security vulnerabilities and improve the overall security of Adobe products and services. Upon receipt of a third-party report, Adobe documents the noted vulnerabilities, evaluates severity and priority, and creates a mitigation strategy or remediation plan. Once the issue is resolved, we re-run the pen tests to ensure the findings have been effectively remediated.
- **Bug Bounty** — Adobe maintains internal and external bug bounty programs. Our internal bug bounties leverage the extensive security talent within the company and help promote application security awareness throughout our engineering teams. In addition, external, crowdsourced, and time-bound pen testing activities leverage the creativity of the Adobe user community and beyond to test our security measures.

## Ticketing and Dashboarding

Automated JIRA ticketing notifies product teams when their service introduces security vulnerabilities or deviates from an acceptable security state so they can promptly mitigate the issue. Using dashboards and key performance indicators (KPIs), the Adobe Application Security team can measure how well the AppSec stack is being adopted across the company as well as determine the effectiveness of our security automation solutions.

# Looking Ahead: The Service Lifecycle (SLC)

The Service Life Cycle (SLC) is the next iteration of the product lifecycle process. SLC is a versatile, unified framework across Adobe's portfolio that provides visibility, consistency, and predictable reviews or executive input into releases, helps ensure alignment across and within business units, and allows flexibility for each business unit to address its own unique requirements.

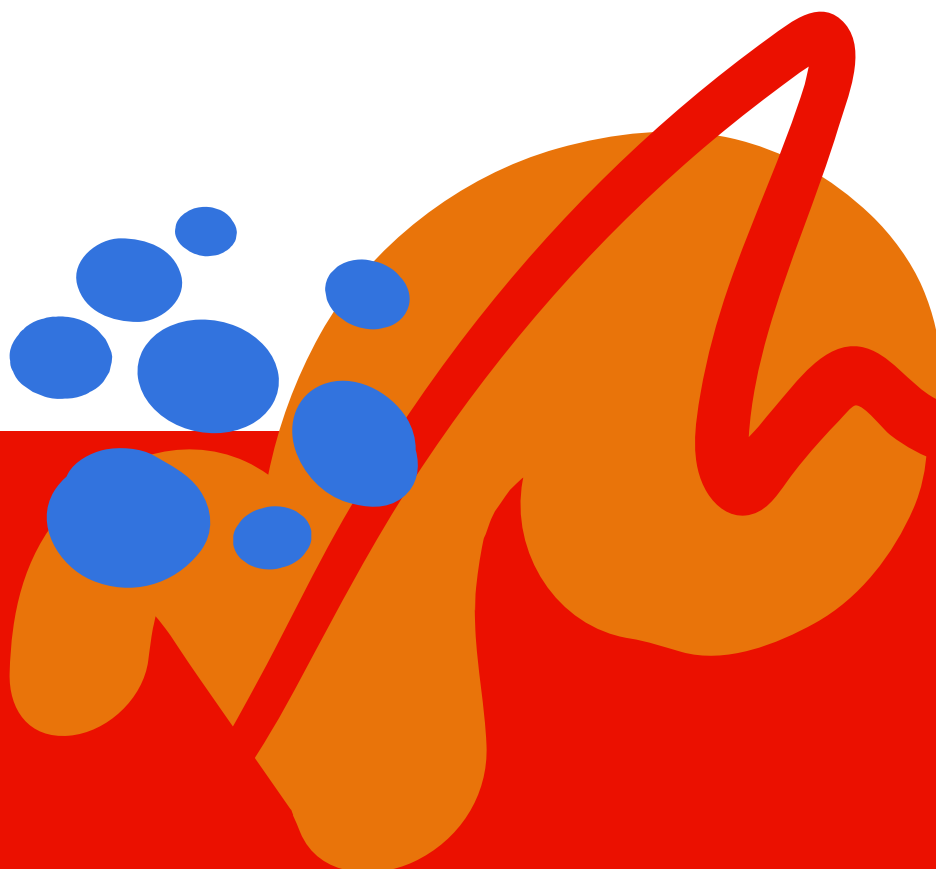


# Conclusion

The Adobe Application Security Stack helps Adobe product and service teams build applications in a "secure-by-default" manner. By focusing on introducing security controls to early in the development cycle and automation, along with continuous monitoring of our security posture through reports, dashboards, and quarterly compliance reviews, the Application Security team helps Adobe proactively prevent security risks and maintain the end-to-end security of both our products and the company's infrastructure.

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative. Further details on the Adobe solution, including SLAs, change approval processes, access control procedures, and disaster recovery processes are available.

Adobe 345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com



Adobe