WHITE PAPER

Adobe Application Security Overview

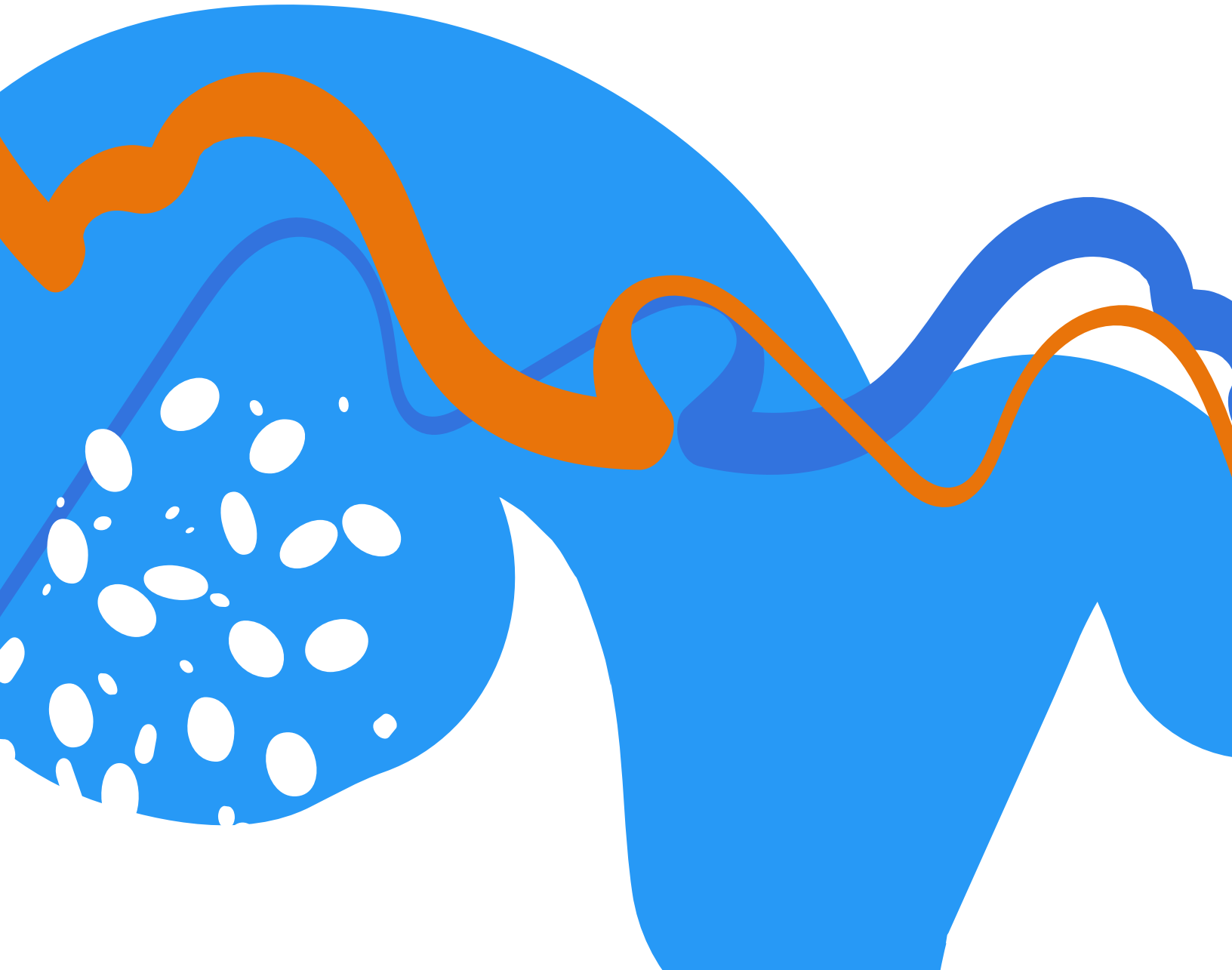
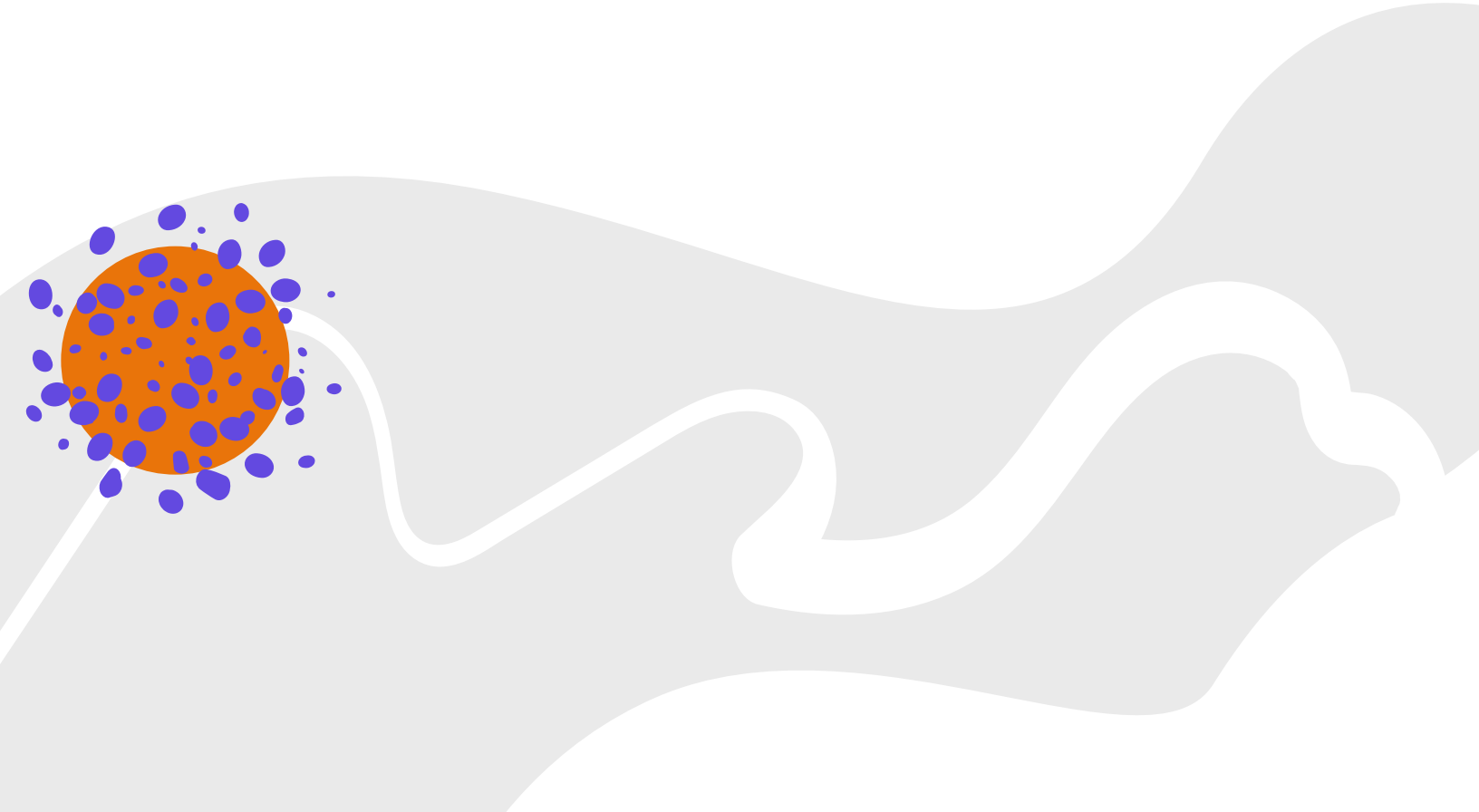


Table of Contents



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. Focused on keeping up with the pace of innovation while helping ensure Adobe products and services include the most effective security measures, our application security team works with product and service teams across the company to build applications in a "secure-by-default" manner. The team also relies on a variety of automation approaches to gather data and help make risk-based decisions that improve the company's overall security posture.

This white paper describes Adobe's 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 reinforce our commitment to modern security practices that protect Adobe and our customers' data and workflows.

The Adobe Application Security Strategy

Adobe's application security strategy focuses on solving security issues at the root cause rather than treating the symptoms. We do this by "shifting left" and introducing security early in the application development lifecycle. By establishing security controls and mechanisms in the requirements, architecture, design, and coding phases of development, we help "bake in" security controls and reduce the high cost of changes introduced during the later testing phases. This approach also minimizes the possibility of actual security risks, which translates to better security for our customers.

The Adobe Secure Product Lifecycle

Integrated into the software product lifecycle—from design and development to quality assurance, testing, and deployment—the Adobe Secure Product Lifecycle (SPLC) serves as the foundation of all security efforts at Adobe. A rigorous set of several hundred security-specific activities, the SPLC defines clear, repeatable processes and capabilities to help our development teams build security into our products and services.

Implemented across the company, the Adobe SPLC controls include roadmaps, security tools, and testing methods that guide the security team in addressing the Open Web Application Security Projects (OWASP) Top 10 most critical application security flaws and the CWE/SANS Top 25 Software Errors. More information about the Adobe SPLC is available on the Adobe Trust Center.

The Adobe Application Security Stack

At Adobe, building secure applications begins with the Application Security Stack. Product teams start by using platforms that are secure-by-default, verify their applications with various automated security capabilities, and weave it all together with security reviews and manual testing.

The three (3) layers in the stack include a range of tools and services based on modern security practices, focused on protecting customer data and workflows, which Adobe product teams can use in their development process to help ensure that security is built into every Adobe application.

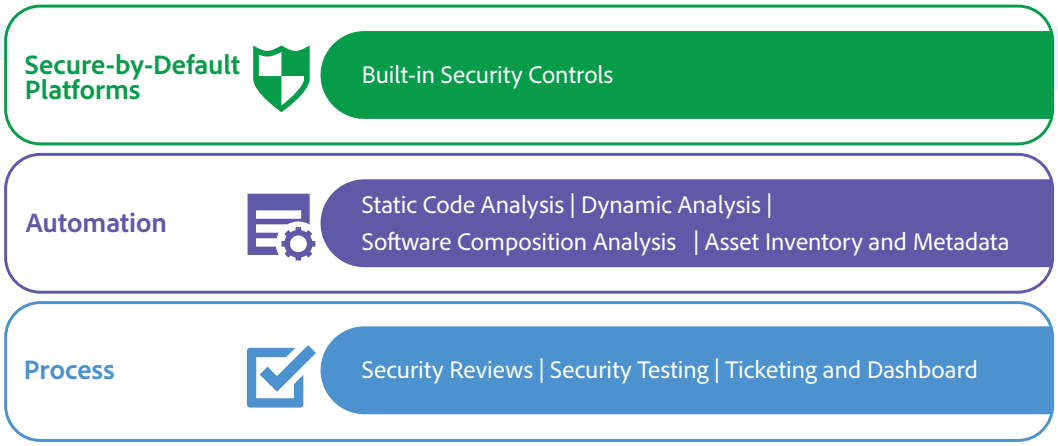


Figure 2: The Adobe Application Security Stack

Secure-By-Default Platforms

Adobe developers use pre-approved secure-by-default platforms to produce well-paved paths that provide development guardrails for the rapid and secure development of Adobe products and services. These guardrails include verified and approved identity and authorization services, API gateway, messaging systems, SDKs, and frameworks.

Secure-by-default platforms not only allow easy scalability, but also help verify the correct implementation of security features and configurations. Based on two main principles—detection and prevention—these platforms include a set of continuous detection solutions to identify possible insecure usage as well as preventive controls that help Adobe developers achieve a secure-by-default posture for their products and services.

Secure-by-default platforms help ensure the following:

- **Secure usage** — By continuously analyzing a vast set of configuration data, logs, and source code, we can quickly identify security misconfigurations in our products and services, discover any deviations, and alert the appropriate product teams.
- **Built-in security controls** — Our investments in security controls that follow best practices, including least privilege, default deny, and built-in authentication, help our product teams focus on their product expertise while protecting customer data and workflows.

Security Automation

At Adobe, automation enables application security to scale across the company and provide continuous security coverage while also keeping 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 platform leverages both open source and commercial tools to scan code repositories. We provide feedback directly to our developers in line with their development workflows, when issues are easiest to mitigate. These tools, along with capabilities unique to our environment, help Adobe deliver the highest possible security in our source code.
- **Dynamic analysis** — Similar to our approach to static code analysis, Adobe uses custom-built and commercial tools to identify security vulnerabilities at runtime.
- **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 our developers, helping ensure timely mitigation.
- **Asset inventory and metadata** — A rich set of company-wide metadata helps our application security team gain deeper insights into Adobe products and services.

Process

Adobe's in-house security expertise and processes form the foundation of our security initiatives. We continually invest in training both our security team members as well as our security champions on emerging technologies and approaches. Ticketing, dashboarding, and effective risk mitigation through adversary intelligence and threat modeling together create the fabric that binds security initiatives into an effective pipeline.

Security Reviews

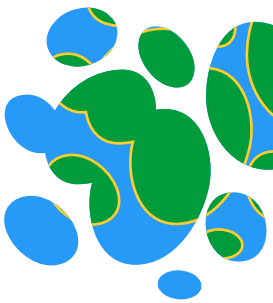
To provide security assurance across Adobe products and services, we engage in in a collaborative process to identify security-related issues, determine the level of associated risk with those issues, and make informed decisions about risk mitigation or acceptance, including:

- **Threat modeling** — Performing a threat model during the design phase helps identify security flaws early in the development lifecycle and creates a strong security foundation for each Adobe product and service. We conduct threat modeling to pinpoint areas in which architectural changes may be required to avoid known threats. Using automation in the threat modeling process helps us scale effectively by automatically generating security requirements, which makes the review process more efficient.
- **Targeted code reviews** — For specific sections of code that deal with sensitive data or for components that are reused by multiple services, our security researchers perform manual code reviews to make sure the code adheres to security best practices.
- **Focused testing** — Adobe security researchers perform regular security tests of our products and services based on multiple factors, including adversary interest and known attack patterns.

Security Testing

In addition to regular security reviews, Adobe conducts penetration testing of our products and services that help strengthen areas of identified weakness and engages our user community with our bug bounty program to detect and report 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 security reviews.
- **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 severities and priorities, and creates a mitigation strategy or remediation plan. Once the issue is resolved, we re-run the penetration tests to help ensure remediation of the issue.
- **Bug bounties** — Adobe maintains internal and external bug bounty programs that reward individuals who discover and report software bugs with public recognition or monetary compensation. Our internal bug bounties leverage security talent within the company and help promote application security awareness throughout our engineering teams. In addition, Adobe leverages the external security researcher community to responsibly disclose exploitable opportunities impacting Adobe or our customers. Responsible disclosure of specific product issues is incentivized by awarding monetary payouts for valid submissions.



Ticketing and Dashboarding

Automated ticketing notifies product teams of known exploited or exploitable security vulnerabilities enabling them to promptly mitigate the issue. Tickets are auto-assigned to teams based on their skills, experience, and product knowledge. Using dashboards and key performance indicators (KPIs), our application security team can measure how well the Adobe Application Security Stack is being adopted across the company, as well as determine the effectiveness of our security automation solutions.

Conclusion

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

Adobe

03/24