

Adobe Security Strategy

Committed to the security and privacy
of your information



Adobe client software is deployed on over 98 percent of the world's desktop and laptop machines as well as on a growing number of mobile and entertainment devices. Adobe software provides a very rich and sophisticated feature set that enables engaging user experiences. However, its ubiquity makes it a popular target for attacks by malicious individuals intent on doing harm.

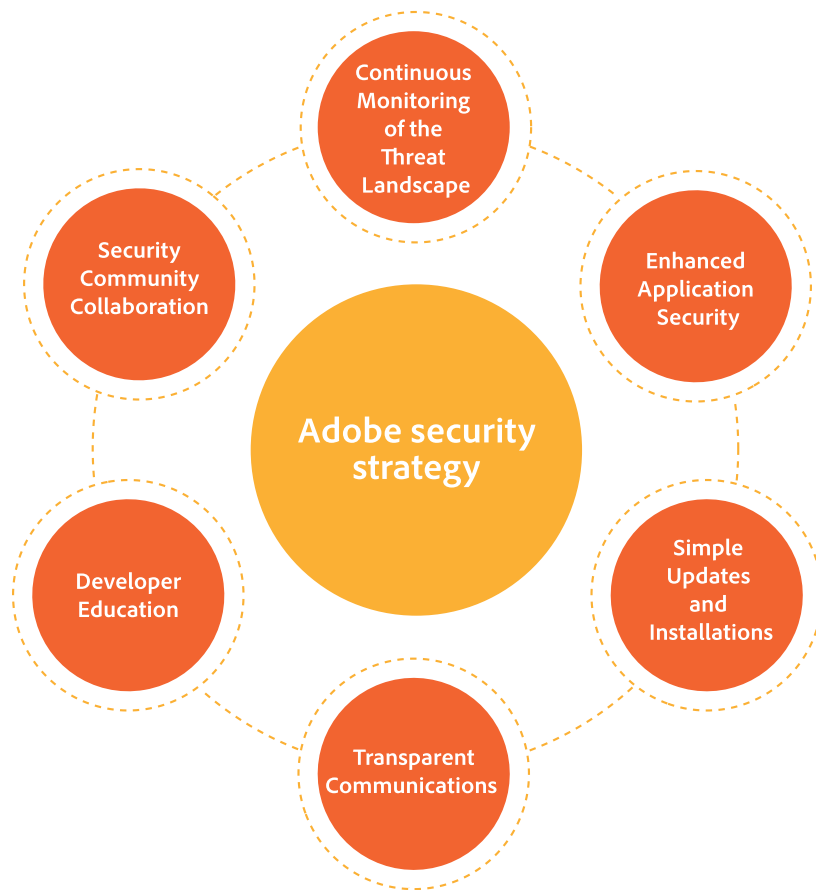
Adobe recognizes that this ubiquity equates to a certain level of trust—and that means we must be persistent and resilient in our pursuit of better product security, continually innovating to help keep you—and your information—safer and more secure.

Committed to security at every level of the organization

Adobe is committed to product security, implementing processes and procedures to improve our responsiveness, information sharing, and support for our customers when incidents occur.

The Adobe Secure Product Lifecycle (SPLC) is at the core of this commitment. The SPLC is a rigorous set of software development best practices, processes, and tools designed to keep your information safer and more secure when you use Adobe software. The SPLC is implemented and driven throughout the Adobe organization by the Adobe Secure Software Engineering Team (ASSET), composed of industry-leading experts in building secure applications who work with our individual product security teams to ensure security is built into every Adobe product before it ships.

Should an incident occur with an Adobe product after it ships, the Adobe Product Security Incident Response Team (PSIRT) is your first line of defense for vulnerability resolution and threat mitigation. Coordinating with the appropriate Adobe product engineering team, PSIRT responds to security issues discovered in Adobe products. PSIRT helps pinpoint, communicate, patch, and remediate the situation as quickly as possible, helping to make sure your valuable information and systems remain safer and more secure.



The Adobe Security Strategy

The Adobe strategic vision for product security includes the following components:

- **Continuous monitoring of the threat landscape**

Adobe is committed to investigating and working with our partners to understand the threats our products face in production environments. To quickly address threats, Adobe continuously monitors the threat landscape and actively engages with security industry partners and customers. This enables us to understand and react to threats as they emerge in and help protect you with near-real-time response.

- **Enhanced application security**

Adobe SPLC is a cutting-edge implementation of security best practices throughout an organization. Our goal is to be a leader in the industry in successfully implementing a secure product lifecycle process. From complete executive support to dedicated security researchers and product security experts across all product teams to our rigorous training and certification process for all engineers, the SPLC provides a model that drives enhanced security capabilities across all of our products.

- **Simple updates and installations**

Adobe understands the significant efforts customers undertake to ensure their computer environment and information remain secure. In today's ever-evolving threat environment, keeping systems updated with the latest security patches is the most critical factor in successful asset protection. Adobe strives to ensure that our security updates are simple, transparent, and predictable, helping you protect your assets more easily and completely. In addition, we are always evolving our updates to meet your changing requirements.

- **Transparent communications**

Adobe strives to be as transparent as possible in our communications to our customers. In terms of product security, this translates to providing as much actionable information as possible—on a regular basis—to our customers. For both regular release cycles and when a security vulnerability or threat is discovered, PSIRT provides the greatest level of transparency to help you reduce your individual risk profile when using Adobe products. Adobe drives several initiatives to simplify how we communicate about security issues as well as how we educate our customers about Adobe product security and security topics in general. Adobe aims to make information about the security of our products and security capabilities easier to find, helping you make better, more informed decisions that can reduce your risk profile.

- **Developer education**

The developer community is a key component of the Adobe ecosystem. Therefore, educating, training, and keeping developers up-to-date on the latest tools and techniques to help them develop more secure products based on the Adobe platform are key priorities. We provide in-depth product education and detailed documentation on all our products, especially Acrobat Reader® and the Adobe LiveCycle® platform. Using the Adobe Developer Connection (ADC), the vast community of Adobe developers can collaborate with each other by sharing best practices, code samples, and so on. Our goal is to help developers reduce the risk profile of their customers.

- **Security community collaboration**

Our involvement and collaboration with security product vendors, standards organizations, and other members of the security ecosystem helps ensure that Adobe products are tightly integrated with the core security infrastructure in your organization, thereby reducing risk and improving overall security. Along with Microsoft, EMC, Nokia, SAP, and Symantec, Adobe is one of the founding members of SafeCode, an organization dedicated to developing standards in product security, integrity, and assurance. Adobe is also a lead member of FIRST (Forum of Incident Response and Security Teams) which encourages cross-industry cooperation to develop better methods and processes to address security incidents. We are integrally involved in OWASP (Open Web Application Security Project), whose mission is to help organizations make informed decisions about true application security risks. Adobe also actively contributes information about its SPLC process to help further development of the models produced by BSIMM (Building Security in Maturity Model).

In addition, Adobe works collaboratively with private security researchers and academic institutions to accelerate innovations in product security, both within our own products as well as other products in the industry, enhancing your overall security and helping to reduce risk.

For more information
www.adobe.com/security



Adobe

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

Adobe, the Adobe logo, Creative Suite, FreeHand, Illustrator, and Macromedia are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Mac OS is a trademark of Apple Inc., registered in the U.S. and other countries. Intel is a trademark of Intel Corporation in the U.S. and other countries. PowerPC is a trademark of International Business Machines Corporation in the United States, other countries, or both. Microsoft, OpenType, Windows, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2010 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

12/10