



SAFECode

Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Adobe Systems Leverages SAFECode as Its Software Delivery Model Evolves



Over the past decade, Adobe Systems has successfully transformed itself from a desktop publishing and graphics editing software vendor to a hosted cloud solutions provider supporting everything from graphic and web design to digital marketing management. Today, Adobe is a global company with nearly \$6 billion in revenue and more than 16,000 employees.


Adobe holds a unique position among software providers; at one time, Adobe Acrobat or Reader were installed on up to 90% of all computers, and Adobe Flash Player was on 99% of all computers. With that massive installed base, Adobe understands better than most its responsibility to delivering software with robust security built in.

The widespread use of Adobe software has made it an attractive target for hackers. Over the past decade, attackers have taken advantage of vulnerabilities in Flash Player and Acrobat Reader on several occasions to infect computers. The company has strived to stay ahead of hackers by taking a vigilant, proactive approach to security. When attackers began to focus on its runtime products, Adobe implemented sandboxing in Acrobat, Acrobat Reader, and Flash Player, which precipitated a steep decline in active exploitation.

The person responsible for leading Adobe's software security efforts is David Lenoe, director of Secure Software Engineering and treasurer, SAFECode. Lenoe began his career in software quality assurance at Macromedia (which was acquired by Adobe in 2005) and has worked in security exclusively for 13 years.

"The value and importance of security has been made crystal clear with a number of high-profile incidents that have occurred across industry and government," said Lenoe. *"That has focused our efforts as a company and helped to raise the visibility and emphasize the importance of the security of our products and services. We make it clear that security is everybody's job, not just the security team's job."*

For Lenoe and his team at Adobe, that job begins with a rigorous training program. *"Adobe created a training program that was used as a basis for the SAFECode training program,"* he said. *"We're always working on new trainings that we push out. The training program allowed us to raise the security IQ within Adobe's developer community, which meant that we didn't have to be in every meeting making sure that security was being addressed. We had advocates within the product teams who could talk about security with a lot of credibility since they were there in the trenches with the rest of the team."*



By organizing the training to follow a progressive, martial arts-style belt system, Lenoe and his team motivated developers to raise their skill levels. *"There's a white belt program, which is a series of introductory, security-101 courses,"* said Lenoe. *"Then there are green, brown, and black belt programs, which are progressively more task- or project-oriented. This system helped us to identify people who are motivated to go above and beyond the white and green belts. That was the starting point for our Security Champion program, which identifies key security drivers within product teams."*

Lenoe points to one technique as being a potent tool in the development of more secure software. *"One investment that we make, which has a really high return, is putting time and resources into threat modeling,"* he noted. *"We spend time with the product teams, helping them to understand their product while learning ourselves about the product, how it functions, where some of the attack surfaces might be, where the most valuable assets are living, and how we can best secure those assets. Threat modeling – and bringing the human element into the picture – are the some of most effective things that we do."*

That focus has enabled Adobe to develop software with better security while evolving its software delivery model. *"We've shifted our focus from a desktop-oriented C++ focused organization to one that's much more focused on hosted services and some of the threats that are faced there,"* he said. *"We've had to acquire knowledge. We've hired experts from the outside who bring that knowledge and have worked in the space for a while. It's a different technology stack. In the desktop world, we had to think about how we could make our updates more accessible to decrease the time between when we released a batch and when it was actually installed and used on the machines. Eventually, for Reader, Acrobat and Flash Player, we settled on a background updater that requires little to no user interaction. Getting from point A to point B took a lot of time and a lot of effort. When we shifted into hosted services, we were able to identify the update cycle as being really important, shrinking that time to push to production to new code, making sure if there's a security fix, we want to be able to push it out as quickly as possible."*

Throughout that evolution, Adobe has relied on SAFECode to help guide its efforts.

"It's been really helpful to work within the working groups at SAFECode on topics like third party components and threat modeling," said Lenoe. *"We've got an interesting buyers and sellers group that talks about how to assess the security of vendors and how to communicate the security of your own products as a vendor. All these working groups are really helpful."*

Sharing information with peers at other companies is another SAFECode benefit.

"Talking to other like-minded people and learning about what they're up to is immensely valuable," he continued. *"I can talk to my counterpart at Dell EMC or at Microsoft if I have a specific problem or question that pops up. SAFECode has also been helpful to us with regards to public policy issues. Talking to policy makers is part of our job as security practitioners. SAFECode gives us a really great vehicle and platform for talking to law makers and their staff. We make trips to Washington DC or Brussels and talk to policy makers as a group. When there are security practitioners who live this job and do the day-to-day work helping to secure software, it's really helpful to share what we're doing and learn how we can be helpful to them as well."*

Those relationships will also help SAFECode stay ahead of emerging threats, according to Lenoe. *"The Internet of Things is an area that's really gaining steam,"* he noted. *"So many companies out there have some kind of connectivity aspect to the work that they're doing. As an organization, we have some IoT practitioners by definition in our midst, but there are a bunch of companies out there who haven't had software development as a focus and who may not know about secure development practices. We have a ton of experience that we can bring to bear as a group. I think it will really help shorten the learning curve and benefit IoT companies who spend time with SAFECode members to become aware of the lessons we've learned and adopt the practices that we're advocating in connection with SAFECode."*

About SAFECode

The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services. Its members include Adobe Systems Incorporated, CA Technologies, EMC Corporation, Intel Corporation, Microsoft Corp., SAP AG, Siemens AG and Symantec Corp. For more information, please visit www.safecode.org.