Adobe® Reader® XI: Improved security and reduced total cost of ownership

Adobe continues to make significant investments in Adobe Reader to help mitigate today's real-world risks while simultaneously reducing the total cost of ownership associated with deployment. Cyber threats are increasingly sophisticated, and protecting intellectual property and networks are a constant concern. Every release of Reader includes new, innovative security enhancements to provide a layered defense against a rapidly changing landscape. Improved update processes and simplified administration also help reduce IT operating expenses. Collectively, the security and deployment improvements in Reader XI enhance security and lower the total cost of ownership for your organization.

Application security

- Protected Mode, an implementation of sandboxing technology, limits the level of access to your system for all PDF files, safeguarding Windows® desktops from malicious code that attempts to write to the file system, delete files, or modify system information. Reader X Protected Mode blocks attackers from installing malware on your system. Reader XI Protected Mode extends this protection by blocking read-only access to your sensitive data.
- Tighter integration with built-in, always-on Windows or Mac OS X security provides additional defense against attacks attempting to control desktop systems or corrupt memory.
- The Adobe PDF Whitelist Framework allows you to selectively enable advanced functionality, such as JavaScript for specific PDF files, sites, or hosts in Windows and Mac OS.
- The Adobe Secure Product Lifecycle process integrates security quality-assurance activities, such as code hardening, threat modeling, and fuzzing, into every phase of Adobe Reader XI development. To learn more, visit *Adobe Security*.

Cumulative, regularly scheduled security updates and patches

- The date of each planned update is pre-announced on the *Adobe PSIRT (Product Security Incident Response Team) blog*. Visit *Adobe Security Bulletins and Advisories* for the current Adobe Reader XI brief.
- Adobe follows a "Patch Tuesday" release schedule to resolve security vulnerabilities accumulated since the previous update. Patch Tuesday is the industry practice of releasing security updates or patches on the second Tuesday of the month.
- Cumulative updates reduce the cost of provisioning new machines or updating machines that skipped the previous update.

Simplified administration

- Support for tools, such as Microsoft SCCM/SCUP, Group Policy Object (GPO) templates, Microsoft App-V, Apple Package Installer, Apple Remote Desktop, and Citrix XenApp, streamline initial deployment and allow the efficient import, publishing, and automation of updates.
- A Multilingual User Interface (MUI) installer rolls out the same worldwide image with a single install job, including all language resources in Windows or Mac OS platforms.
- Free tools, such as the Customization Wizard XI, Enterprise Toolkit (ETK) for Adobe Acrobat® and Reader, provide greater control over enterprise-wide deployments (see *Enterprise Administration*).

PDF viewers are now part of the everyday business workflow. Today, Adobe Reader XI offers the most advanced features to help secure and protect your data. Adobe encourages customers with security assurance requirements to accelerate their upgrade plans to Adobe Reader XI to benefit from these improvements.

To learn more about Adobe Reader XI, visit *Adobe Reader Security*. To learn more about the Acrobat Family, visit *PDF Solutions for IT*.

6/12