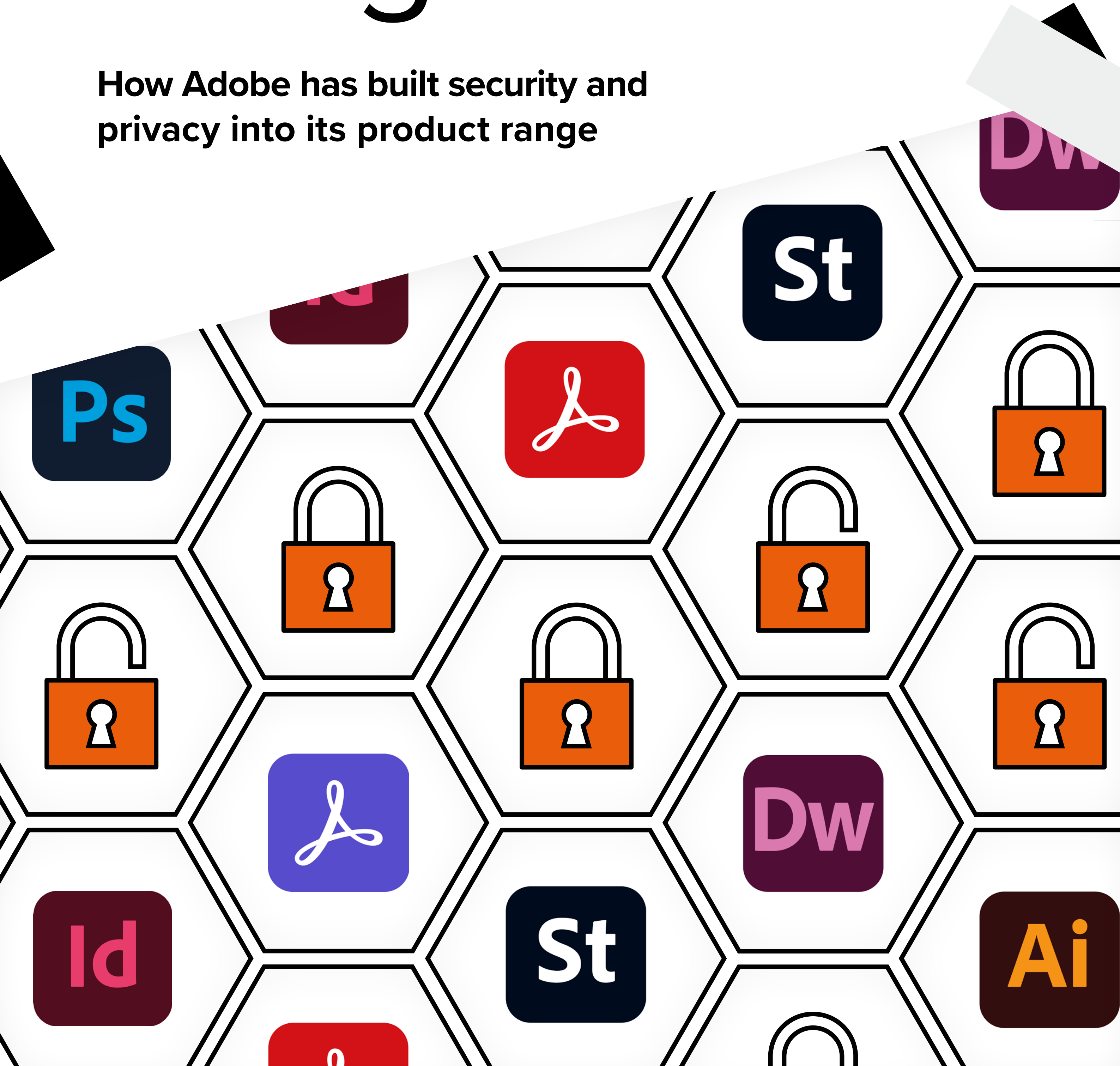
Adobe

JIGSAW24

Secure by design

How Adobe has built security and privacy into its product range



Introduction

The recent growth in remote working has accelerated the move from localised storage to cloud computing. This brings with it huge benefits for business, with employees able to work together in real time from any location. Equally, employers benefit too thanks to reduced server maintenance, fewer software updates and lower associated costs.

However, it has also put the issue of security to the top of the agenda for many, with many employees now able to access content and data on a range of devices, whether they're at home, at the workplace, or travelling.

Fortunately, Adobe recognises the importance of security for its customers and Creative Cloud was built to protect your company's creative assets and data. Not only this, but it is also very easy to license and manage – all through the Adobe Admin Console.

This whitepaper gives you a rundown of the security-based workflows available within Adobe tools and highlights the advanced security measures Adobe takes to ensure its industry-leading software continues to protect its enterprise users' assets and data.

Experience matters

Adobe's security practices are rooted in more than 25 years of experience working with digital documents. In addition to this, Adobe constantly invests heavily in providing comprehensive and proven security measures, including participating in the Microsoft Active Protections Program.

As part of the Adobe Software Security Certification Program, Adobe trains its development teams in security knowledge and, through the Adobe Common Control Framework (CCF), Adobe created a set of security activities and compliance controls that are applied throughout its product operations teams and infrastructure and application teams.

Adobe also implements strict technical controls and restrictions on employees' access to customer data, along with thorough background checks, employee termination procedures, high facility security levels, virus protection and customer data confidentiality across all its employees and offices around the world – all to protect the company itself from security threats.

Security at the heart

Adobe's tools have security built into them from the outset. For example, content stored in the Document Cloud is encrypted by default, access control to shared assets is in your hands, and all Adobe tools have security at their heart with features such as password lockout procedures and Federated IDs with Single Sign-On.

Enhanced workflows

The security features within Adobe's tools also allow for streamlined and secure workflows. Acrobat DC enables secure collaboration with a spectrum of document security options, from basic password security to certificate-based controls. Adobe Sign, for example, allows users to send, sign, track, and manage signature processes smoothly, making document signing fast, easy, and secure.

The Admin Console

The Adobe Admin Console helps businesses organise their entire Adobe entitlements from one easy-to-access location – providing everything you need and enabling simple account and user management in an instant.

From here, you can access an account overview, track your licenses, assign products to users and groups, download packages and view insights, as well as edit account details and settings, and manage users and storage across your organisation.

Adobe Acrobat

Acrobat is another versatile asset of Adobe's, giving you all the tools you need to keep your projects moving on the go, without compromising on security.

Wherever your teams are and whatever device they're using, Acrobat makes workflows smooth. It is the world's foremost PDF solution, used by millions, and enables you to do everything you need – from converting PDFs, scanning to PDF, and organising pages and documents, to editing, commenting, sharing and signing your documents quickly and safely.

As previously mentioned, with Adobe Sign, you can manage end-to-end signing processes with ease, with security measures applied to the whole process and documents certified with a tamper-evident seal. Alternatively, documents can be signed with certificate-based digital signatures from trusted service providers on either the Adobe Approved Trust List (AATL) or the European Union Trusted List (EUTL) – widely regarded as a secure way of electronic document signing.

Access control

Your security is Adobe's priority when it comes to storing and sharing your content on the Document Cloud.

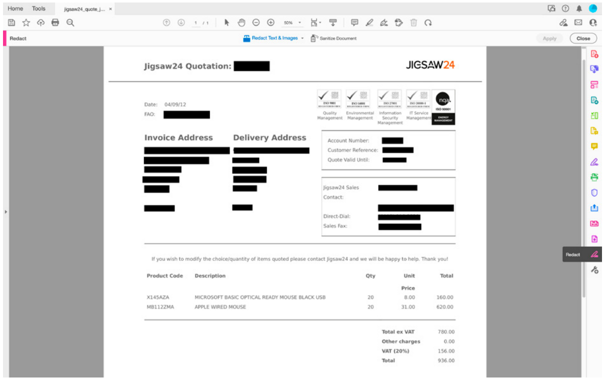
Users can easily control access by applying passwords and permissions to PDF documents to prevent any changes and restrict printing, copying, or alterations. And by default, all Document Cloud files are private and visible only to the end user who uploaded them, unless explicit actions are taken.

Content sharing is straightforward too, however, completed via a link shared with the recipient(s). Content can be shared as either Review – which allows the recipient to make comments, but not edit or alter the document – or View Only – which allows the recipient to view the document in a read-only format.

Adobe also puts the power in your hands when it comes to controlling how content is shared externally, with restrictive settings available to limit employees from sharing documents in certain ways, such as restricting invitation-based sharing to recipients in the claimed, trusted, and whitelisted domains.

True redaction

With Adobe Acrobat DC, users can permanently delete both text and graphic images, as well as search and redact based on patterns, including phone numbers, credit card numbers and email addresses. This way, confidential or sensitive information can be completely removed, rather than just masked. Thanks to the sanitise document feature, even hidden information and non-graphic elements like metadata can also be completely removed.



Jigsaw24 Quotation: [redacted]

Date: 04/09/12
FAO: [redacted]

Invoice Address
[redacted]

Delivery Address
[redacted]

Account Number: [redacted]
Customer Reference: [redacted]
Quote Valid Until: [redacted]

Jigsaw24 Sales Contact: [redacted]
[redacted]
Direct-Dial: [redacted]
Sales Fax: [redacted]

If you wish to modify the choice/quantity of items quoted please contact Jigsaw24 and we will be happy to help. Thank you!

Product Code	Description	Qty	Unit Price	Total
X145AZA	MICROSOFT BASIC OPTICAL READY MOUSE BLACK USB	20	8.00	160.00
MB112ZMA	APPLE WIRED MOUSE	20	31.00	620.00

Total ex VAT	780.00
Other charges	0.00
VAT (20%)	156.00
Total	936.00

Sandboxing

Sandboxing is a security measure that helps to protect computer systems from malicious code that attempts to write or read from a system via PDF files. With this measure, the execution environment of untrusted files (all PDFs are treated as potentially corrupt by default) is automatically confined to a restricted sandbox.

Adobe leverages industry-leading sandboxing technology, known as Protected Mode in Acrobat Reader DC and Protected View in Acrobat DC. Measures include improved security hardening with more proactive sandboxing, as well as leak protection and code sanitation.

The result is a high level of protection for users' sensitive data and intellectual property, safeguarding your systems against a range of malicious attacks.

Protected View works like Protected Mode but is built for the Rich Acrobat DC feature set and protects against read as well as write-based attacks. Protected View runs in both ways users open a PDF document – in Acrobat DC or in a browser – and on Windows 8 and above, it always runs in an AppContainer, providing an even stronger defence. And to enable all Acrobat DC features, all you need to do is click the Enable All Features button and the file will be trusted in future.

Secure storage

All components of Adobe Document Cloud services are hosted in accordance with industry-standard practices and undergo regular industry-recognised certifications and audits. Electrical, mechanical, and life support systems and equipment are constantly monitored, with ongoing preventative maintenance taking place. High levels of physical and environmental controls are in place across storage centres, including backup power, disaster recovery, incident response, climate control and fire suppression procedures.

Adobe also works with streamlined patching systems and actively monitors Adobe Document services using industry-standard intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).

Multi-layered encryption

By default, all data and assets are encrypted with unique AES 256-bit symmetric security keys, while an additional layer of control can be applied to Adobe Document Cloud files using a dedicated encryption key managed by the AWS KMS and automatically rotated on an annual basis.

Secure product lifecycle

Only Adobe offers the Secure Product Lifecycle – a unique, time-tested suite of security practices that govern everything from multi-layered software architecture to data privacy, access control, and more. As part of the Adobe SPLC, development teams take part in ongoing security training and certification, keeping the security knowledge of those working on Adobe products and services at the highest possible level.

Contact us

If you would like more information on making your business workflow secure with Adobe, you can speak to our Adobe experts on **03332 409 204** or email us at **adobe@Jigsaw24.com**.