Überblick über die Sicherheit von Adobe Acrobat DC mit Document Cloud-Services.

Inhalt.

Für Adobe Sign gelten separate Sicherheitsmaßnahmen, auch wenn Adobe Sign zu den PDF-Services von Document Cloud gehört.

Zusammenfassung.

Adobe nimmt die Sicherheit eurer digitalen Inhalte ernst. Sicherheitsmaßnahmen sind ein fester Bestandteil unserer Software-Entwicklung, Prozesse und Programme. Sie werden von interdisziplinären Teams konsequent umgesetzt, um etwaigen Zwischenfällen vorzubeugen, diese aufzudecken und angemessen darauf zu reagieren. Darüber hinaus halten wir uns durch Kooperation mit Partnern, Experten und anderen Unternehmen über aktuelle Bedrohungen und Schwachstellen auf dem neuesten Stand und integrieren fortlaufend hochentwickelte Sicherheitstechnologien in unsere Produkte und Services.

Adobe-Services, die mit Kundeninhalten in Berührung kommen, sind für zahlreiche Branchenstandards zertifiziert. Online findet ihr eine Liste der Zertifizierungen, Standards und gesetzlichen Vorgaben, die Produkte und Lösungen von Adobe erfüllen, sowie Informationen zur DSGVO-Compliance.

In diesem Whitepaper erfahrt ihr, welchen Stellenwert Sicherheit bei Adobe Acrobat DC, Adobe Acrobat Reader DC, Adobe Document Cloud, Services von Adobe Document Cloud und den zugehörigen Daten hat.

Überblick über Acrobat DC mit Document Cloud-Services.

Acrobat DC umfasst die aktuelle Version von Acrobat auf dem Desktop, Premium-Funktionen für Acrobat Reader als Mobile App und Online-Services von Document Cloud – für produktive, vernetzte, durchgängig sichere Abläufe auf jedem Gerät. Mit Acrobat DC und Services von Document Cloud können Kunden Inhalte in elektronische Dateien umwandeln und weitergeben. Darüber hinaus können sie über Cloud-Services, Desktop-Software oder Mobile Apps PDF-Dateien erstellen und bearbeiten.

Dokumentensicherheit.

Schwärzung.

Mit den Schwärzungswerkzeugen von Acrobat DC lassen sich vertrauliche Informationen zuverlässig schützen. Sowohl Text als auch Bilder können vor der Weitergabe eines Dokuments unwiderruflich gelöscht werden. Ihr könnt auch Inhalte suchen und entfernen, die bestimmten Mustern entsprechen, beispielsweise Telefonnummern, Kreditkartennummern und E-Mail-Adressen. Während andere Tools und Methoden der Schwärzung Inhalte lediglich verdecken, werden bei Acrobat DC die ausgewählten Informationen vollständig aus der Datei entfernt. Mit der Funktion „Dokument bereinigen“ lassen sich auch verborgene Informationen wie Metadaten aus einem PDF-Dokument entfernen.

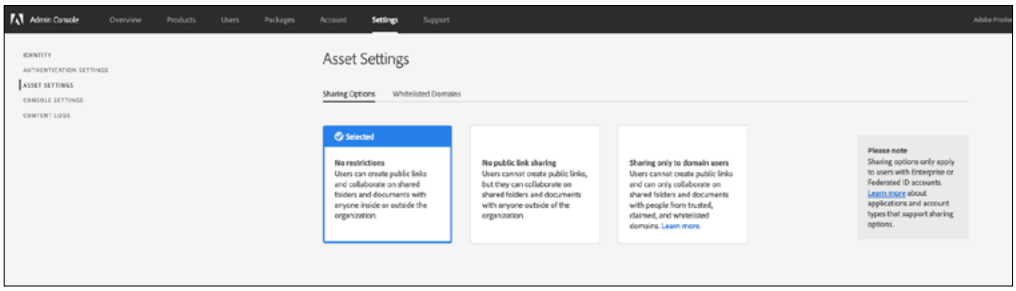
Freigabe.

Bei Document Cloud gespeicherte Dateien werden automatisch als privat gekennzeichnet. Ihr Inhalt ist somit nur für den Anwender sichtbar, der sie hochgeladen hat. Ein Endanwender muss die Freigabe von Inhalten aktiv veranlassen, ansonsten bleiben sie privat. Die Freigabe von Document Cloud-Dateien erfolgt über den Versand eines Links per E-Mail, Textnachricht oder Software für Zusammenarbeit.

Dateien können über Document Cloud-Services entweder zum Anzeigen oder zur Überprüfung freigegeben werden. Ist „Kommentare zulassen“ bei der Freigabe deaktiviert, kann der Empfänger über den erhaltenen Link nur eine schreibgeschützte Fassung des Inhalts abrufen. Ist die Option aktiviert, kann der Empfänger Kommentare anbringen, aber keine Änderungen am Inhalt der PDF-Datei vornehmen.

Elementeinstellungen und Einschränkungen für Freigaben.

Über die Elementeinstellungen hat eine Organisation die Kontrolle darüber, wie Mitarbeiter Inhalte extern weitergeben können. Der IT-Administrator kann mit einer einzigen Einstellung die Nutzung bestimmter Freigabefunktionen von Document Cloud einschränken. Er kann zum Beispiel festlegen, dass nur Personen aus vertrauenswürdigen, beanspruchten und zugelassenen Domains auf Einladung hin auf freigegebene Dateien zugreifen dürfen. Wenn diese Richtlinie in Kraft ist, können Mitarbeiter unternehmenseigene Inhalte nicht an externe Personen weitergeben, deren Domains per Definition der Richtlinie nicht zugelassen sind.



Microsoft Information Protection (MIP).

Dateien, die durch MIP-Lösungen wie Azure Information Protection (AIP) und AIP für Microsoft 365 geschützt sind, können mit Acrobat DC oder Acrobat Reader DC geöffnet werden. Weitere Informationen erhaltet ihr auf der Microsoft-Website unter Was ist Azure Information Protection?

Geschützter Modus in Acrobat Reader DC.

Um euch vor Schad-Software zu schützen, die versucht, mithilfe von PDF-Dateien das Dateisystem eurer Computer zu manipulieren, bietet Adobe seit Adobe Reader X den geschützten Modus, eine Implementierung der Sandbox-Technologie.

Beim Sandboxing handelt sich um eine Methode, eine abgegrenzte Umgebung mit eingeschränkten Rechten für die Ausführung von Programmen zu schaffen. Die Sandbox trägt zum Schutz des Endanwender-Systems vor Angriffen mit nicht vertrauenswürdigen Dokumenten bei, die möglicherweise ausführbaren Code enthalten. Im Kontext von Acrobat Reader DC gelten alle PDF-Dateien und die Prozesse, die sie aufrufen, als nicht vertrauenswürdige Inhalte. Acrobat Reader DC behandelt alle PDF-Dokumente als potenziell schädlich und beschränkt alle Prozesse, die die PDF-Datei aufruft, auf die Sandbox.

In Acrobat Reader DC wehrt der geschützte Modus Angreifer ab, die versuchen, Schad-Software auf dem Anwendersystem zu installieren. Der Schutz trägt dazu bei, das Auslesen und den Abruf vertraulicher Daten und geistigen Eigentums auf einem Computer oder im Firmennetzwerk zu verhindern. Der geschützte Modus wird standardmäßig beim Starten von Acrobat Reader DC aktiviert. Insbesondere schränkt dieser Modus die Zugriffsrechte für das Programm ein, sodass Microsoft Windows-Systeme vor böswilligen PDF-Dateien geschützt werden, die gegebenenfalls versuchen, in das Dateisystem des Computers zu schreiben oder Informationen auszulesen, Dateien zu löschen oder auf andere Weise Systemdaten zu verändern.

Der geschützte Modus kann unter Windows 8 und höher in einem AppContainer ausgeführt werden, was die Abschirmung der Umgebung zusätzlich verbessert.

Geschützte Ansicht in Acrobat DC.

Ähnlich wie der geschützte Modus von Acrobat Reader DC ist die geschützte Ansicht von Acrobat DC eine Implementierung der Sandbox-Technologie. Bei Acrobat DC werden in dieser Ansicht nicht nur das Schreiben von schadhaftem Code auf einem Computer-System mithilfe einer PDF-Datei unterbunden, sondern auch das Auslesen vertraulicher Daten oder geistigen Eigentums.

Die geschützte Ansicht beschränkt die Ausführung nicht vertrauenswürdiger Programme (beispielsweise eine PDF-Datei mit von ihr aufgerufenen Prozessen) auf eine isolierte Umgebung – die „Sandbox" –, um zu verhindern, dass schädlicher Code in der Datei den Rechner beeinträchtigt. Bei der geschützten Ansicht wird davon ausgegangen, dass alle PDF-Dateien potenziell schädlich sind. Daher wird jede Ausführung auf die Sandbox beschränkt, es sei denn, eine Datei wurde als vertrauenswürdig gekennzeichnet.

Dieser Schutz beim Öffnen von PDF-Dokumenten steht sowohl in Acrobat DC als auch im Browser zur Verfügung. Die geschützte Ansicht wird unter Windows 8 und höher in einem AppContainer ausgeführt. Dadurch entsteht eine noch besser abgeschirmte Umgebung.

Oben im Anzeigefenster wird eine Meldungsleiste eingeblendet, sobald der Anwender eine potenziell schädliche Datei in der geschützten Ansicht öffnet. Diese Leiste weist darauf hin, dass eine nicht vertrauenswürdige Datei in der geschützten Ansicht geöffnet wurde, in der viele Acrobat DC-Funktionen deaktiviert und die Möglichkeiten der Interaktion mit der Datei eingeschränkt sind. Die Datei ist schreibgeschützt. Eingebettete oder verknüpfte schädliche Inhalte können in euer System nicht eindringen.

Um die Datei als vertrauenswürdig zu kennzeichnen und alle Funktionen von Acrobat DC zu aktivieren, klickt der Anwender auf der Meldungsleiste auf „Alle Funktionen aktivieren". Acrobat schaltet daraufhin die geschützte Ansicht aus und fügt die Datei zur Liste vertrauenswürdiger Quellen bzw. Elemente hinzu. Ab dem nächsten Öffnen dieser Datei gelten nicht mehr die Einschränkungen der geschützten Ansicht.

Architektur der Document Cloud-Services.

Document Cloud bietet folgende Services:

- **Seiten verwalten** – Seiten in einem PDF-Dokument einfügen, löschen, neu anordnen oder drehen
- **PDF-Dateien erstellen** – Word-, Excel- und PowerPoint-Dokumente sowie Bilder oder Fotos in PDF-Dateien umwandeln
- **PDF-Dateien exportieren** – PDF-Dokumente in editierbare Microsoft Word-, Excel-, PowerPoint- oder RTF-Dateien umwandeln
- **PDF-Dateien bearbeiten** – PDF-Dokumente auf dem Desktop, Smartphone oder Tablet bearbeiten
- **Dateien kombinieren** – Mehrere Dateien zu einem kompakten PDF-Dokument zusammenführen – auf jedem Gerät
- **Senden und verfolgen** – Dokumente zuverlässig versenden, den Status verfolgen und sich über alle Aktionen informieren lassen
- **Adobe Scan** – Fotos von Quittungen und anderen Papierdokumenten in editierbare, hochwertige PDF-Dateien umwandeln
- **Adobe Sign** – Dokumente zur sicheren, rechtlich bindenden, elektronischen Unterzeichnung vorbereiten und versenden – auf jedem Gerät

Sicherheit der Document Cloud-Services.

Berechtigungen und Identitäts-Management.

IT-Administratoren gewähren Endanwendern Zugriff auf Document Cloud-Services über die Admin Console per anwendergebundene Lizenz. Document Cloud unterstützt drei ID-Typen für anwendergebundene Lizenzen:

- Die **Adobe ID** ist ein von Adobe gehosteter und von Einzelanwendern erstellter und verwalteter Account. Über die Adobe ID kann nur dann auf Services von Document Cloud zugegriffen werden, wenn ein IT-Administrator den Zugriff gewährt.
- Die **Enterprise ID** ist ein von Adobe gehosteter und vom IT-Administrator des Abonnenten erstellter und verwalteter Account. Die Organisation ist Eigentümer der Anwender-Accounts und aller zugehörigen Inhalte.
- Die **Federated ID** ist ein vom Unternehmen verwalteter Account, bei dem alle Identitätsprofile vom internen Identitäts-Management-System über Single Sign-on (SSO) bereitgestellt werden. Sämtliche Accounts sowie die zugehörigen Inhalte werden von der IT erstellt und verwaltet. Adobe unterstützt die meisten Anbieter für SAML 2.0-Authentifizierung.

Die meisten Unternehmen verwenden eine Enterprise ID oder eine Federated ID für interne und externe Mitarbeiter. Dazu müssen diese Personen eine E-Mail-Adresse mit der firmeneigenen E-Mail-Domain haben, da darüber Berechtigungen und anwendergenerierte Inhalte verwaltet werden können. Weitere Informationen zu den ID-Typen findet ihr auf der Adobe-Website unter Einrichten der Identität.

Für die Kennwortspeicherung für Adobe IDs und Enterprise IDs wird der Hash-Algorithmus SHA 256 in Kombination mit Kennwort-Salts und einer Vielzahl an Hash-Iterationen verwendet. Die von Adobe gehosteten Accounts werden kontinuierlich auf ungewöhnliche Aktivitäten hin überprüft, um das Sicherheitsrisiko zu minimieren. Kennwörter für Federated ID-Accounts werden nicht von Adobe verwaltet. Weitere Informationen findet ihr im englischsprachigen Whitepaper über die Sicherheit von Adobe Identity Management Services.

Elektronische Unterschriften und digitale Signaturen.

Die Document Cloud-Services umfassen zwei verschiedene Werkzeuge für die sichere Arbeit mit Unterschriften:

- **Ausfüllen und unterschreiben** auf Basis von Adobe Sign ermöglicht lückenlose elektronische Unterzeichnungsprozesse, die Gesetzen und Bestimmungen zu elektronischen Unterschriften in den USA, der Europäischen Union und den meisten anderen Industrieländern entsprechen. Anwender können Unterschriften einholen, Unterschriftsprozesse nachverfolgen sowie unterzeichnete Dokumente und Prüfprotokolle automatisch archivieren. Der gesamte Prozess wird von effektiven Sicherheitsmaßnahmen begleitet. Zusätzlich werden Dokumente und Prüfprotokolle mit einem Siegel vor Manipulation geschützt.

Auf Smartphones und Tablets wird die Nachverfolgung des Dokumentenstatus nicht unterstützt. Weitere Informationen zu Adobe Sign und entsprechenden Sicherheitsfunktionen findet ihr im technischen Überblick über Adobe Sign.

- **Zertifikate** ermöglichen das Unterzeichnen mit zertifikatbasierten digitalen IDs von Anbietern von der Adobe Approved Trust List (AATL) oder den European Union Trusted Lists (EUTL). Das Unterzeichnen mit einer zertifikatbasierten ID, die von einer Zertifizierungsstelle vergeben wurde, gilt allgemein als eine der sichersten Methoden für die elektronische Unterzeichnung von Dokumenten. Die ID wird dem Unterzeichner eindeutig zugeordnet und kann seine Identität bestätigen. Im Unterzeichnungsprozess wird das Zertifikat des Unterzeichners mithilfe des nur ihm zugewiesenen privaten Schlüssels an das Dokument gebunden.

Acrobat DC stellt automatisch eine Verbindung zu einer Zertifizierungsstelle her, um die Signatur des Unterzeichners und die Authentizität des unterzeichneten Dokuments zu prüfen. Diese Form der Signatur erfüllt die Standards für elektronische Unterschriften in PDF-Dokumenten, darunter PAdES (PDF Advanced Electronic Signature), Teil 2, 3 und 4, und die JITC*-konforme Verschlüsselung und Verwendung einer PKI (Public Key Infrastructure) mit AES-256, RSA-4096, SHA512 oder RSA-PSS. Zudem können Anwender mit dem Werkzeug „Zertifikate“ Dokumenten Zeitstempel hinzufügen und sie mit einem manipulationssicheren Siegel versehen.

Document Cloud-Speicher.

IT-Administratoren können Enterprise ID- und Federated ID-Accounts über die Adobe Admin Console zwar persönlichen Cloud-Speicher zuteilen, sie haben aber keinen direkten Zugriff auf Dateien, die Anwender bei Document Cloud speichern. Nach dem Löschen eines Enterprise ID- oder Federated ID-Accounts mit Speicher für Shared Services verlieren alle betreffenden Endanwender den Zugriff auf Daten und Inhalte, die sie unter diesen IDs in der Cloud gespeichert haben. Die Daten der Anwender werden nach 90 Tagen gelöscht.

IT-Administratoren können über die Admin Console auch Adobe ID-Accounts Speicherplatz zuteilen. Sie können Adobe ID-Accounts zwar nicht löschen, aber sie können ihnen das Zugriffsrecht für den Cloud-Speicher des Abonnenten sowie für Programme und Services entziehen. In dem Fall werden Dateien, die der betreffender Anwender in der Cloud gespeichert hat, nach 90 Tagen gelöscht.

Document Cloud-Services nutzen die mehrmandantenfähige Speicherung. Inhalte von Kunden werden von einer EC2-Instanz (Amazon Elastic Compute Cloud) verarbeitet und in S3-Buckets (Amazon Simple Storage Service) sowie über eine MongoDB-Instanz auf einem Amazon Elastic Block Store (EBS) gespeichert. Die Inhalte selbst werden in Amazon S3-Buckets gespeichert, und die Metadaten zu den Inhalten in EBS über MongoDB. Der Zugriff erfolgt über IAM-Rollen (Identity and Access Management) innerhalb der jeweiligen AWS-Region (Amazon Web Services).

Metadaten und Elemente werden mit 256-Bit-AES-Verschlüsselung auf Amazon EBS-Volumes gespeichert. Dabei werden FIPS 1402-konforme (Federal Information Processing Standards) kryptografische Algorithmen verwendet, die der NIST-Empfehlung 80057 (National Institute of Standards and Technology) entsprechen.

Daten werden in mehreren Rechenzentren und in jedem Rechenzentrum auf mehreren Geräten redundant gespeichert. Der gesamte Netzwerkverkehr wird einer systematischen Datenprüfung sowie Prüfsummenberechnungen unterzogen, um Daten zu schützen und ihre Integrität sicherzustellen. Die Inhalte werden schließlich synchron und automatisch in anderen Rechenzentren innerhalb der Region des Kunden repliziert, um auch bei Datenverlust an zwei Standorten die Datenintegrität aufrechtzuerhalten.

*Joint Interoperability Test Command des US-Verteidigungsministeriums

Weitere Informationen zu den genannten Amazon-Services findet ihr unter:

- MongoDB
- Amazon S3
- AWS Key Management Service (KMS)
- Amazon EC2

Dedizierter Verschlüsselungsschlüssel.

In Amazon S3-Buckets gespeicherte Inhalte werden standardmäßig mit symmetrischen 256-Bit-AES-Sicherheitsschlüsseln verschlüsselt, die für jeden Kunden und jede in Anspruch genommene Domain einzeln vergeben werden. Über einen dedizierten Verschlüsselungsschlüssel, der von AWS KMS verwaltet und jährlich automatisch geändert wird, können IT-Administratoren eine zusätzliche Kontroll- und Sicherheitsebene für einige oder alle Domains ihres Unternehmens implementieren.

Dieser dedizierte Verschlüsselungsschlüssel kann über die Admin Console deaktiviert werden. Danach können Endanwender nicht mehr auf Inhalte zugreifen, die mit diesem Schlüssel verschlüsselt wurden, und auch keine Inhalte hoch- oder herunterladen.

Hinweis: Document Cloud-Dateien lassen sich mit dem dedizierten Verschlüsselungsschlüssel verschlüsseln, Metadaten aber nicht.

Weitere Informationen zur Verschlüsselung mit einem dedizierten Schlüssel findet ihr auf den folgenden Adobe-Hilfeseiten:

- Verwalten der Verschlüsselung
- Häufige Fragen zu dedizierten Verschlüsselungsschlüsseln

Amazon Web Services.

Wie zuvor erwähnt, werden alle Komponenten von Document Cloud-Services bei AWS in den USA gehostet, einschließlich Amazon EC2 und Amazon S3. Amazon EC2 ist ein Webservice, der automatisch skalierbare Rechenkapazität in der Cloud bereitstellt und damit die Web-Skalierung vereinfacht. Amazon S3 ist eine anerkannt zuverlässige Infrastruktur für die Speicherung und den Abruf jeder beliebigen Datenmenge.

Die AWS-Plattform stellt Services bereit, die mit branchenüblichen Sicherheitsverfahren im Einklang stehen. AWS wird regelmäßig branchenweit anerkannten Zertifizierungsmethoden und Prüfungen unterzogen. Weitere Informationen zu AWS und den Sicherheitsmaßnahmen bei Amazon findet ihr unter AWS Cloud Sicherheit.

Verantwortungsbereiche von AWS und Adobe.

AWS betreibt, verwaltet und überwacht die Komponenten von der Hypervisor-Virtualisierungsebene bis hin zur physischen Sicherheit der Räumlichkeiten, in denen Document Cloud-Services ausgeführt werden. Adobe ist seinerseits verantwortlich für das Gast-Betriebssystem und deren Verwaltung (einschließlich Updates und Sicherheits-Patches), für Programme und für die Konfiguration der von AWS bereitgestellten Firewall für die Sicherheitsgruppe.

AWS betreibt zudem die Cloud-Infrastruktur, die von Adobe genutzt wird, um verschiedene Rechenressourcen beispielsweise für Datenverarbeitung und -speicherung zur Verfügung zu stellen. Die AWS-Infrastruktur umfasst die Räumlichkeiten, das Netzwerk, die Hardware und die Software (beispielsweise das Host-Betriebssystem oder Virtualisierungs-Software), die die Provisionierung und Verwendung dieser Ressourcen ermöglichen. Amazon wendet in den Bereichen Entwicklung und Verwaltung von AWS branchenübliche Verfahren an und erfüllt zahlreiche Sicherheitsstandards.

Sichere Verwaltung.

Adobe verwendet Secure Shell (SSH) und Secure Sockets Layer (SSL) für Verbindungen zur Verwaltung der AWS-Infrastruktur.

Geografischer Standort von Kundendaten im AWS-Netzwerk.

Alle anwendergenerierten Inhalte, die bei Document Cloud hochgeladen werden, werden in regionalen Rechenzentren von AWS USA Ost (Nord-Virginia) gespeichert. Backups der Inhalte erfolgen innerhalb des jeweiligen Rechenzentrums sowie zur besseren Lastenverteilung und aus Gründen der Redundanz in weiteren Rechenzentren innerhalb der Region.

Geografischer Standort von ID-Daten im AWS-Netzwerk.

ID-Daten werden zur Lastenverteilung in mehreren AWS-Rechenzentren in Virginia (USA Ost), Oregon (USA West), Irland (EU) und Singapur (Asien-Pazifik) gespeichert und in allen Rechenzentren repliziert. Adobe erfüllt alle gesetzlichen Anforderungen an grenzüberschreitende Datentransfers. Details hierzu findet ihr auf der Adobe-Website unter Grenzüberschreitende Datenübertragungen.

Isolation von Kundendaten/Abgrenzung von Kunden.

AWS wendet strenge Sicherheits- und Kontrollmechanismen zur Mandantenisolation an. AWS ist eine virtualisierte, mehrmandantenfähige Umgebung (Multi-Tenant-Umgebung). Sie hat Sicherheits-Management-Prozesse und andere Sicherheitskontrollfunktionen implementiert, durch die jeder Kunde von anderen AWS-Kunden isoliert wird. Per IAM schränkt Adobe den Zugriff auf Rechen- und Speicherinstanzen noch weiter ein.

Sichere Netzwerkarchitektur.

Mithilfe von Firewalls und anderen Mechanismen überwacht und kontrolliert AWS die Kommunikation an der Außengrenze sowie an wichtigen internen Grenzen des Netzwerks. Diese Mechanismen wenden Regelsätze, Access Control Lists (ACLs) und Konfigurationen an, um den Informationsfluss zu speziellen Informationssystem-Services zu lenken. ACLs bzw. Richtlinien für den Netzwerkfluss dienen zur gezielten Steuerung des Verkehrsflusses an jeder verwalteten Schnittstelle.

Amazon Information Security prüft und genehmigt alle ACL-Richtlinien und weist sie mithilfe des ACL-Manage-Tools von AWS automatisch jeder verwalteten Schnittstelle zu. So ist sichergestellt, dass diese die jeweils aktuellen ACLs anwenden.

Netzwerküberwachung und -schutz.

Mit einer Reihe von automatisierten Überwachungssystemen stellt AWS eine hohe Performance und Verfügbarkeit aller Services sicher. Überwachungswerkzeuge helfen, an Netzwerkpunkten mit ein- und ausgehender Kommunikation ungewöhnliche oder unzulässige Aktivitäten und Situationen zu erkennen. Das AWS-Netzwerk bietet zuverlässigen Schutz vor traditionellen Problemen der Netzwerksicherheit:

- DDoS-Angriffe (Distributed Denial Of Service)
- MITM-Angriffe (Man in the Middle)
- IP-Spoofing
- Port-Scanning
- Packet-Sniffing durch andere Instanzen

Weitere Informationen zu Netzwerküberwachung und -schutz findet ihr unter AWS Cloud Sicherheit.

Intrusion Detection.

Adobe überwacht Document Cloud-Services mithilfe von IDS-Lösungen (Intrusion Detection System) und IPS-Systemen (Intrusion Prevention Systems).

Protokolle.

Adobe führt eine Server-seitige Protokollierung der Aktivitäten von Nutzern der Document Cloud-Services durch, um Service-Ausfälle, spezielle Kundenprobleme und gemeldete Fehler zu beheben. In den Protokollen werden Adobe IDs nur zur Behebung spezieller Kundenprobleme gespeichert. Sie enthalten keine Kombinationen aus Benutzername und Kennwort. Nur technisches Support-Personal sowie ausgewählte Techniker und Entwickler von Adobe mit entsprechender Berechtigung haben Zugriff auf die Protokolle, um spezielle Probleme zu beheben.

Überwachung der Service-Qualität.

AWS überwacht alle elektrischen, technischen und Notfallsysteme und -einrichtungen, damit Probleme mit den Services unmittelbar erkannt werden. Um den unterbrechungsfreien Betrieb aller Geräte sicherzustellen, sorgt AWS für eine kontinuierliche Wartung.

Datenspeicherung und -sicherung.

Adobe speichert alle Daten von Document Cloud-Services in Amazon S3, das über eine Speicherinfrastruktur mit hoher Beständigkeit verfügt. Um die Beständigkeit zu erhöhen, speichert Amazon S3 die Kundendaten über PUT- und COPY-Aktionen synchron an mehreren physischen Standorten. Objekte werden redundant auf mehreren Geräten an mehreren physischen Standorten in einer Amazon S3-Region gespeichert.

Amazon S3 berechnet Prüfsummen für sämtlichen Netzwerkverkehr, um eine eventuelle Beschädigung von Datenpaketen beim Speichern oder Abruf von Daten zu erkennen. Die Datenreplikation für Amazon S3-Datenobjekte erfolgt innerhalb des regionalen Clusters, in dem die Daten gespeichert sind. Es findet keine Replikation in Cluster der Rechenzentren anderer Regionen statt.

Die Replizierung von Metadaten erfolgt über Snapshots von Amazon EBS-Volumes, die nach einem ähnlichen Prinzip wie Amazon S3-Datenobjekte gespeichert werden. Weitere Informationen zum Thema Sicherheit bei AWS findet ihr unter AWS Cloud Sicherheit.

Änderungs-Management.

Routinemäßige und notfallbedingte Änderungen sowie Konfigurationsänderungen an der bestehenden AWS-Infrastruktur werden von AWS entsprechend den Branchenstandards für gleichartige Systeme autorisiert, protokolliert, getestet, genehmigt und dokumentiert. AWS wird von Amazon nach einem festen Zeitplan aktualisiert, um mögliche Auswirkungen für Kunden zu minimieren. AWS informiert die Kunden per E-Mail oder über das AWS Service Health Dashboard, falls die Nutzung des Service beeinträchtigt sein sollte. Den aktuellen Systemstatus von Document Cloud können Kunden auf der Adobe-Website prüfen.

Patch-Management.

AWS ist verantwortlich für die Installation von Patches auf Systemen, die die Bereitstellung von AWS-Services wie dem Hypervisor und Netzwerk-Services unterstützen. Adobe übernimmt die Installation von Patches für eigene Gast-Betriebssysteme, Software und Programme, die in AWS ausgeführt werden. Sind Patches erforderlich, stellt Adobe anstatt des Patches eine neue, sichere Instanz des Betriebssystems bzw. des Programms zur Verfügung.

Physische Sicherheit und Umgebungssicherung bei AWS.

Die Maßnahmen zur Erhöhung der physischen Sicherheit und zur Umgebungssicherung bei AWS werden in SOC-Berichten (Service Organization Controls), Typ 1 und Typ 2, beschrieben. Im folgenden Abschnitt sind einige Sicherheitsmaßnahmen und Kontrollmechanismen aufgeführt, die in AWS-Rechenzentren weltweit angewandt werden. Ausführlichere Informationen zum Thema Sicherheit bei AWS findet ihr unter AWS Cloud Sicherheit.

Physische Sicherheit.

Die AWS-Rechenzentren verwenden branchenübliche Architekturen und Technologien. AWS-Rechenzentren sind in unauffälligen Gebäuden untergebracht. Der physische Zugang wird durch professionelles Sicherheitspersonal, Videokameras, Einbruchmeldeanlagen und andere elektronische Geräte kontrolliert. Das gesamte Gelände und alle Gebäudeeingänge werden überwacht. Autorisierte Mitarbeiter müssen mindestens zwei Mal eine Zwei-Faktor-Authentifizierung durchlaufen, bevor sie die einzelnen Etagen des Rechenzentrums betreten dürfen. Alle Besucher und Dienstleister müssen sich ausweisen und registrieren. Sie werden während der gesamten Besuchszeit von autorisierten Mitarbeitern begleitet.

Der Zugang zum Rechenzentrum und zu Informationen wird ausschließlich Mitarbeitern und Dienstleistern gestattet, die einen legitimen geschäftlichen Grund haben. Besteht dieser geschäftliche Grund nicht mehr, wird die Zutrittsberechtigung sofort aufgehoben, auch wenn die jeweilige Person weiterhin als Mitarbeiter von Amazon oder Amazon Web Services tätig ist. Der Zutritt zu den Rechenzentren durch Mitarbeiter von AWS wird protokolliert und regelmäßig überprüft.

Brandbekämpfung.

AWS hat Anlagen zur automatischen Branderkennung und -bekämpfung eingerichtet. Die Brandmeldeanlage setzt sich aus folgenden Komponenten zusammen: Rauchmelder, die in allen Räumlichkeiten des Rechenzentrums installiert sind, Räume für die mechanische und elektrische Infrastruktur, Kühlräume und Räume für die Generatoranlage. Diese Bereiche werden entweder durch Nasssprinkleranlagen, doppelt gesicherte vorgesteuerte Sprinkleranlagen oder Trockensprinkleranlagen geschützt.

Raumklima und -temperatur.

Mit einer Klimaanlage sorgt AWS für eine konstante Betriebstemperatur der Server und anderer Hardware-Geräte. So wird eine Überhitzung verhindert und die Gefahr von Ausfällen verringert. In den Rechenzentren von AWS werden die atmosphärischen Bedingungen auf einem optimalen Niveau gehalten. Temperatur und Luftfeuchtigkeit werden vom AWS-Personal und den technischen Systemen entsprechend überwacht und geregelt.

Kontinuierliche Stromversorgung.

Die Stromversorgungssysteme der Rechenzentren von AWS sind vollständig redundant und können rund um die Uhr instand gehalten werden, ohne Betriebsabläufe zu beeinträchtigen. Durch eine unterbrechungsfreie Stromversorgung (USV) ist während eines Stromausfalls die Stromversorgung von kritischen und wichtigen Geräten sichergestellt. In den Rechenzentren ermöglichen Generatoren eine Notstromversorgung in der gesamten Anlage.

Disaster Recovery.

AWS-Rechenzentren zeichnen sich durch eine hohe Verfügbarkeit aus und sind so konzipiert, dass System- oder Hardware-Ausfälle nur minimale Auswirkungen auf die Kunden haben. Die Rechenzentren sind in Gruppen auf mehrere Regionen weltweit verteilt, rund um die Uhr online und für Kunden jederzeit verfügbar. Bei einem Funktionsausfall wird der Datenverkehr automatisch umgeleitet.

Für wichtige Programme gilt die N+1-Konfiguration. Kommt es in einem Rechenzentrum zu einem Funktionsausfall, stehen genügend Kapazitäten zur Verfügung, damit der Datenverkehr auf die anderen Standorte verteilt werden kann. Weitere Informationen zur Disaster Recovery-Richtlinie von AWS findet ihr unter AWS Cloud Sicherheit.

Risiko- und Schwachstellen-Management bei Adobe.

Unser Ziel sind kurze Reaktionszeiten, erfolgreiche Risikominderung und effektive Fehlerbehebung. Im Rahmen des Risiko- und Schwachstellen-Managements überwachen wir die aktuelle Bedrohungslage, tauschen Informationen mit Sicherheitsexperten auf der ganzen Welt aus, beheben Vorfälle innerhalb kürzester Zeit und leiten sämtliche Informationen an unsere Entwickler-Teams weiter. So erzielen wir für alle Adobe-Produkte die größtmögliche Sicherheit.

Penetrationstests.

Adobe beauftragt führende Sicherheitsunternehmen mit der Durchführung von Penetrationstests, um potenzielle Sicherheitslücken aufzudecken und die Sicherheit von Produkten und Services von Adobe insgesamt zu verbessern. Nach Erhalt des Berichts eines Drittanbieters dokumentiert Adobe die Sicherheitslücken, bewertet deren Schweregrad und Priorität und entwirft eine Strategie zur Risikominimierung oder einen Plan zur Problembehebung. Adobe führt einmal im Jahr einen umfassenden Penetrationstest und jeden Monat Schwachstellen-Scans durch.

Einmal pro Quartal und vor jedem Release führt das Sicherheits-Team für Document Cloud eine Risikoeinschätzung aller Komponenten und Services durch. Das Sicherheits-Team für Document Cloud arbeitet gemeinsam mit den Leitern für Technik/IT und Entwicklung vor jedem Release an der Behebung aller riskanten Schwachstellen. Weitere Informationen zu den Penetrationstests findet ihr im englischsprachigen Whitepaper zum Thema Sicherheit in der Entwicklung bei Adobe.

Problembehandlung und Benachrichtigung.

Jeden Tag werden neue Sicherheitslücken und Bedrohungen erkannt. Adobe reagiert so schnell wie möglich darauf. Neben branchenspezifischen Schwachstellenlisten, die unter anderem von US-CERT (United States Computer Emergency Readiness Team), Bugtraq und SANS herausgegeben werden, erhält Adobe regelmäßig die neuesten Sicherheitshinweise führender Anbieter von Sicherheitslösungen.

Weitere Informationen zu diesem Thema findet ihr im englischsprachigen Whitepaper über den Umgang mit Zwischenfällen bei Adobe.

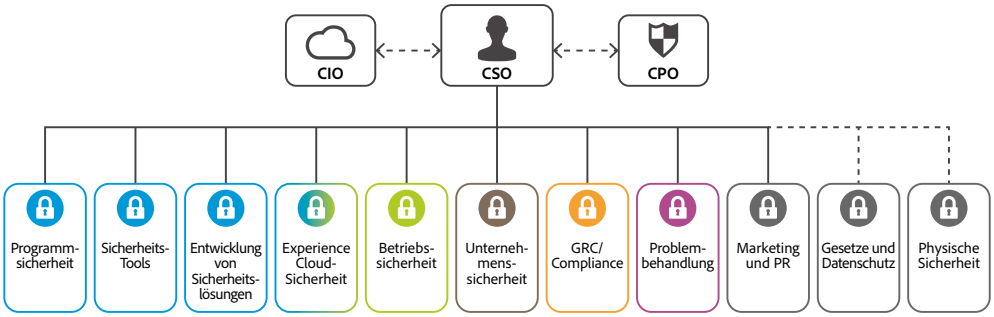
Forensische Analyse.

Bei der Untersuchung von Vorfällen verwendet das Document Cloud-Team den forensischen Analyseprozess, der ein vollständiges Image bzw. ein Speicherabbild des/r betroffenen Rechner(s), eine sichere Beweisaufbewahrung sowie eine lückenlose Dokumentation der Überwachungskette umfasst.

Die Adobe-Sicherheitsorganisation.

Sämtliche Maßnahmen zur Erhöhung der Sicherheit der Produkte und Services von Adobe werden vom Chief Security Officer (CSO) koordiniert. Das Büro des CSO ist für alle Sicherheitsinitiativen für Produkte und Services sowie die Implementierung von Adobe Secure Product Lifecycle (SPLC) zuständig.

Der CSO leitet auch das Adobe Secure Software Engineering Team (ASSET), ein zentrales Team von Sicherheitsexperten, die den Produkt- und Entwickler-Teams von Adobe, unter anderem dem Document Cloud-Team, beratend zur Seite stehen. Die ASSET-Experten arbeiten mit verschiedenen Produkt- und Entwickler-Teams von Adobe zusammen, um bei allen Produkten und Services das gewünschte Maß an Sicherheit zu erreichen. Sie empfehlen Sicherheitsmaßnahmen mit klar strukturierten und reproduzierbaren Prozessen in den Bereichen Entwicklung, Bereitstellung, Betrieb und Fehlerbehebung.



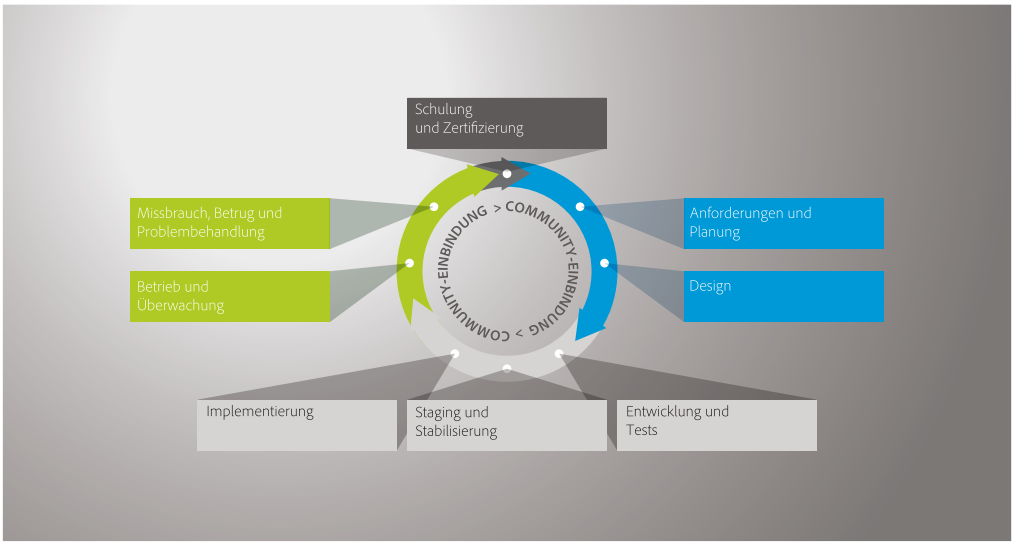
Entwicklung sicherer Adobe-Produkte.

Wie bei anderen wichtigen Produkten und Services von Adobe wird für Document Cloud der SPLC-Prozess (Adobe Secure Product Lifecycle) angewandt. Das SPLC-Programm von Adobe umfasst zahlreiche spezielle, auf größtmögliche Sicherheit ausgerichtete Methoden, Prozesse und Werkzeuge, die während des gesamten Produktzyklus zum Einsatz kommen – von Design und Entwicklung bis hin zu Qualitätssicherung, Test und Bereitstellung. Die Sicherheitsexperten des ASSET geben im Rahmen des SPLC-Programms nach Bewertung potenzieller Sicherheitsrisiken Empfehlungen für einzelne Produkte und Services. Das Programm wird unter anderem durch die regelmäßige Einbindung der Community kontinuierlich weiterentwickelt und ist somit in Bezug auf Technologien, Sicherheitsmethoden und Bedrohungen stets auf dem neuesten Stand.

Adobe Secure Product Lifecycle.

Die Adobe SPLC-Aktivitäten umfassen, je nach betroffener Document Cloud-Komponente, einige oder alle der folgenden empfohlenen Verfahren, Prozesse und Werkzeuge:

- Sicherheits-Training und -zertifizierung für die Produkt-Teams
- Analyse der Produktsicherheit, Risiken und aktuellen Bedrohungen
- Richtlinien, Regeln und Analysen für sicheres Coden
- Service-Leitfäden, Sicherheitswerkzeuge und Testmethoden, mit denen das Sicherheits-Team für Document Cloud die vom Open Web Application Security Project (OWASP) veröffentlichten Top 10 schwerwiegender Sicherheitslücken von Web-Programmen und die von CWE/SANS veröffentlichten 25 gefährlichsten Software-Fehler leichter erkennen und vermeiden kann
- Prüfungen der Sicherheitsarchitektur und Penetrationstests
- Prüfung des Quell-Codes zur Behebung von Fehlern, die Sicherheitslücken verursachen können
- Validierung anwendergenerierter Inhalte
- Scannen von Programmen und Netzwerken
- Beurteilung der Produktreife, Notfallpläne, Veröffentlichung von Unterlagen für Entwickler



Adobe Software Security Certification Program.

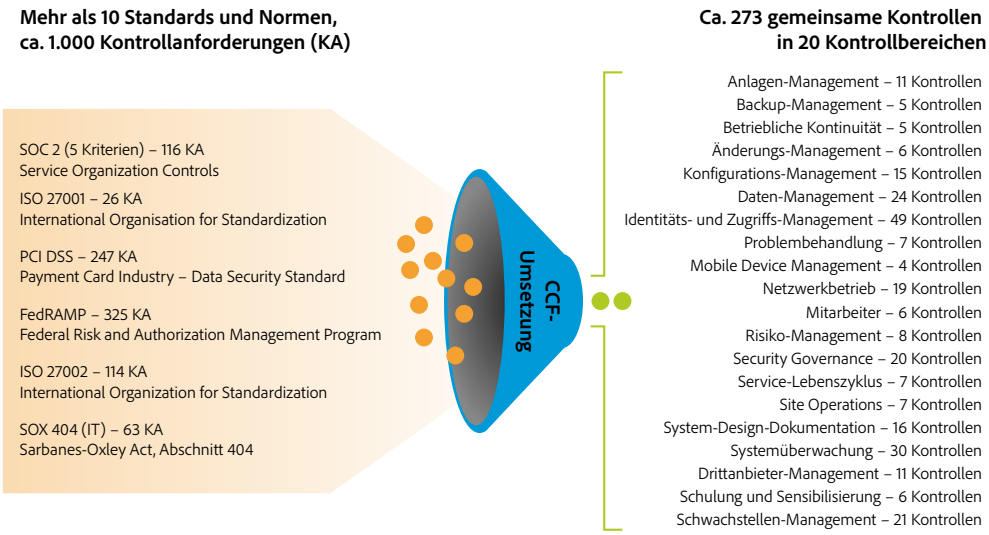
Im Rahmen des Adobe Secure Product Lifecycle führt Adobe regelmäßig Sicherheits-Trainings für Entwickler-Teams im gesamten Unternehmen durch, um Mitarbeiter auf dem neuesten Stand zu halten. Mitarbeiter, die am Adobe Software Security Certification Program teilnehmen, können durch den Abschluss von Sicherheitsprojekten verschiedene Stufen erreichen. Weitere Informationen zu unseren Sicherheitspraktiken findet ihr im englischsprachigen Whitepaper zum Thema Sicherheit in der Entwicklung bei Adobe.

Weitere Informationen zum Adobe Software Security Certification Program findet ihr im englischsprachigen Whitepaper zur Sicherheitskultur bei Adobe.

Document Cloud-Services und Compliance.

Das Adobe Common Controls Framework (CCF) umfasst eine Reihe von Sicherheitsmaßnahmen und Compliance-Kontrollen, die in den Produkt-Teams sowie in verschiedenen Teilen der Infrastruktur- und Programm-Teams im Einsatz sind.

Bei der Entwicklung des CCF hat Adobe die Kriterien der gängigsten Sicherheitszertifikate für Cloud-basierte Unternehmen analysiert. Mehr als 1.000 Anforderungen wurden in Adobe-spezifische Kontrollmechanismen umgesetzt, die etwa einem Dutzend Branchenstandards entsprechen.



Aktuelle Informationen zu den Zertifizierungen und zur Compliance von Adobe Acrobat DC mit Document Cloud-Services findet ihr online im Adobe Trust Center.

Informationen zur Compliance von Adobe Sign findet ihr im technischen Überblick über Adobe Sign.

Letztendlich trägt der Kunde die Verantwortung dafür, dass gesetzliche Auflagen eingehalten werden, Adobe-Lösungen seine Compliance-Anforderungen erfüllen und angemessen gesichert sind.

Adobe-Mitarbeiter.

Adobe hat Mitarbeiter und Niederlassungen auf der ganzen Welt. Die folgenden Prozesse und Vorgehensweisen werden zum Schutz vor Sicherheitsbedrohungen unternehmensweit angewendet.

Mitarbeiterzugriff auf Kundendaten.

Für Document Cloud verwendet Adobe segmentierte Entwicklungs- und Produktionsumgebungen, bei denen der Zugriff auf Live-Produktionssysteme auf Netzwerk- und Programmebene durch technische Kontrollen begrenzt wird. Die Mitarbeiter verfügen über spezifische Autorisierungen für den Zugriff auf Entwicklungs- und Produktionssysteme. Mitarbeiter ohne legitimen geschäftlichen Grund können nicht auf diese Systeme zugreifen.

Zuverlässigkeitsprüfung.

Adobe führt vor jeder Neueinstellung eine Zuverlässigkeitsprüfung durch. Inhalt und Umfang des Berichts, den Adobe in der Regel einfordert, umfassen Fragen zum Bildungshintergrund, den beruflichen Werdegang, Gerichtsakten einschließlich etwaiger Vorstrafen sowie berufliche und private Referenzen – jeweils im Rahmen des geltenden Rechts. Die Zuverlässigkeitsprüfung entspricht der regulären Vorgehensweise in den USA zur Einstellung neuer Mitarbeiter. Hierzu gehören unter anderem Bewerber, die Systeme verwalten oder Zugriff auf Kundendaten haben werden. Neue Mitarbeiter in Zeitarbeit unterliegen in den USA der Zuverlässigkeitsprüfung durch die jeweilige Zeitarbeitsfirma. Diese muss den Richtlinien zur Zuverlässigkeitsprüfung von Adobe entsprechen. Außerhalb der USA führt Adobe bei bestimmten neuen Mitarbeitern Zuverlässigkeitsprüfungen gemäß den Richtlinien von Adobe und dem im jeweiligen Land geltenden Recht durch.

Kündigung von Mitarbeitern.

Wenn ein Mitarbeiter bei Adobe kündigt, reicht sein Vorgesetzter ein Kündigungsformular ein. Nach der Genehmigung informiert Adobe People Resources alle Beteiligten per E-Mail über spezielle Maßnahmen, die bis zum letzten Tag des Mitarbeiters zu ergreifen sind. Kündigt Adobe einem Mitarbeiter, sendet Adobe People Resources eine ähnliche E-Mail-Benachrichtigung an alle Beteiligten, in der auch Datum und Uhrzeit der Kündigung angegeben sind.

Adobe Corporate Security stellt anhand der folgenden Maßnahmen sicher, dass der Mitarbeiter nach dem letzten Beschäftigungstag keinen Zugang mehr zu vertraulichen Dateien oder Büros von Adobe hat:

- Löschung des E-Mail-Zugriffs
- Löschung des Remote-VPN-Zugriffs
- Entwertung der Zugangskarte für das Büro und das Rechenzentrum
- Aufhebung des Netzwerkzugriffs

Auf Anfrage können Vorgesetzte den Sicherheitsdienst bitten, den gekündigten Mitarbeiter aus dem Büro oder Gebäude von Adobe zu begleiten.

Physische Sicherheit.

An jedem Unternehmensstandort von Adobe sind rund um die Uhr Sicherheitskräfte im Einsatz. Adobe-Mitarbeiter tragen eine Schlüsselkarte mit ID für den Zugang zum Gebäude mit sich. Besucher betreten das Gebäude nur über den Haupteingang, melden sich an der Rezeption an und ab, zeigen einen temporären Besucherausweis vor und werden von einem Mitarbeiter begleitet. Alle Server-Komponenten, Entwicklungsrechner, Telefonsysteme, Datei- und Mailserver sowie andere sensible Systeme sind zu jeder Zeit in kontrollierten Server-Räumen eingeschlossen, die nur von entsprechend autorisiertem Personal betreten werden dürfen.

Virenschutz.
Adobe scannt alle eingehenden und ausgehenden geschäftlichen E-Mails auf bekannte Malware.

Vertraulichkeit von Kundendaten.
Adobe behandelt Kundendaten vertraulich. Die Nutzung oder Weitergabe der im Auftrag eines Kunden erfassten Daten durch Adobe erfolgt ausschließlich im Rahmen des mit diesem Kunden abgeschlossenen Vertrags und entsprechend den Nutzungsbedingungen und Datenschutzrichtlinien von Adobe.

Fazit.
Das proaktive Sicherheitskonzept und die strikten Verfahren, die in diesem Whitepaper beschrieben wurden, dienen dem Schutz von Acrobat DC, Acrobat Reader DC, Document Cloud-Services und euren vertraulichen Daten. Adobe nimmt die Sicherheit eurer digitalen Inhalte ernst. Die weltweiten Bedrohungen werden fortlaufend beobachtet, um kriminellen Aktivitäten stets einen Schritt voraus zu sein und die Sicherheit der Kundendaten zu gewährleisten.

Weitere Informationen findet ihr online im Adobe Trust Center.

Adobe

Adobe Systems GmbH
Georg-Brauchle-Ring 58
D-80992 München
Adobe Systems (Schweiz) GmbH
World Trade Center
Leutschenbachstrasse 95
CH-8050 Zürich
www.adobe.de, www.adobe.at,
www.adobe.ch, www.adobe.com

8/21