



# ERSTE SCHRITTE MIT DIGITALER RECHTEVERWALTUNG FÜR ONLINEVIDEO

Kunden nutzen Onlinevideo auf einer Vielzahl an Geräten – von Smartphones und Tablets bis hin zu PCs und internetfähigen Fernsehgeräten. Daher benötigen Publisher eine Möglichkeit, ihren Content vor Piraterie und jeglicher Art von nicht autorisierten Zugriffen zu schützen. Die digitale Rechteverwaltung (DRM) liefert die Kontrolle, die Publisher zum Schutz ihres Contents für unterschiedlichste Geschäftsmodelle und verschiedene Verbreitungsstrategien benötigen.

Diese Kurzdarstellung bietet Antworten auf häufig gestellte Fragen zur DRM und verdeutlicht die Rolle der DRM bei der Contentsicherheit. Zudem soll dieses Dokument Ihnen die Entscheidung erleichtern, wie Sie DRM am besten in Ihre Onlinevideostrategie einbinden.

## Benötige ich DRM?

### Was genau ist DRM?

Die digitale Rechteverwaltung (DRM) umfasst Technologien, die Contenteigentümern das Sichern ihres Contents, einschließlich Premiumcontent und nicht öffentlichen, internen Contents, ermöglichen. Zudem können mit der DRM Richtlinien für die Interaktion von Konsumenten mit dem Content festgelegt werden. Diese betreffen beispielsweise Zahlungsbedingungen, zugelassene Geräte und ob den Benutzern das Kopieren und Freigeben Ihres Contents erlaubt wird. DRM ist das Hauptinstrument für Herausgeber von Onlinevideos zum Schutz vor nicht autorisierter Verwendung, Piraterie und sonstigen Verstößen gegen die Nutzungsbedingungen.

### Warum sollte ich meinen Content schützen?

DRM ist nicht mehr ausschließlich für große Medienunternehmen wie Sender, Filmstudios und Plattenfirmen geeignet. Onlinevideo hat den Mainstream erobert, und so produzieren verschiedenste Organisationen hochwertigen Markencontent, den die Publisher schützen und über dessen Verbreitung sie die Kontrolle behalten möchten.

Wenn Sie Premiumcontent – von kurzen und langen Unterhaltungsvideos bis hin zu im Handel erhältlichen Trainingsvideos – veröffentlichen und verbreiten, sollten Sie eine Möglichkeit haben, Ihr Zahlungsmodell anzuwenden und sicherzustellen, dass Ihre Kunden Ihr Umsatzpotenzial nicht durch das Kopieren oder Freigeben Ihrer Videos an nicht autorisierte Zuschauer einschränken.

Selbst Publisher, die keinen kostenpflichtigen Videocontent bereitstellen, müssen ihren Content schützen, damit er nicht von nicht autorisierten Parteien missbräuchlich genutzt wird. Beispiele dafür sind proprietärer Content eines Unternehmens, vertrauliche Behördeninformationen, interne Ankündigungen, Kommunikationen mit Partnern oder Kanälen sowie sonstiger nicht öffentlicher Content. Solche Videos sind möglicherweise sehr nützlich für das Erfüllen interner geschäftlicher Anforderungen – aber auch potenziell schädigend, wenn sie unangemessen aufgerufen oder freigegeben werden. Sie würden es sicher nicht zulassen, dass ein Fremder Ihre Server durchstöbert und sich an Ihren Daten und Ihrem geistigen Eigentum bedient. Ihr Videocontent sollte ebenso geschützt werden.

## Wie funktioniert DRM?

### Welche unterschiedlichen Arten von DRM gibt es?

Es gibt zwei unterschiedliche Arten von DRM: **Anonym** und **erweitert**.

**Anonyme DRM** (auch als nicht authentifizierte DRM bezeichnet) sichert den Content am Ursprungsort (z. B. am Speicherplatz im Content Delivery Network vor dem Transport des Contents) und ermöglicht Ihnen, Richtlinien zur Anzeige und Verbreitung für diesen Content festzulegen. Die anonyme DRM ist eine Notwendigkeit für alle Publisher, um kostenfreien, nicht öffentlichen Content vor nicht autorisierten Zugriffen zu schützen und zudem geeignet für die Unterstützung vieler Premiumcontentmodelle.

Lösungen wie Adobe Flash Access bieten eine sofort einsatzbereite Lösung für anonyme DRM, da jedes Video einschließlich Metadaten und Richtlinien am Ursprungsort gesichert und verschlüsselt wird, um die optimale Sicherheitskontrolle für Flash-unterstützte Umgebungen zu gewährleisten.

**Erweiterte DRM** liefert eine noch höhere plattformübergreifende Contentkontrolle, z. B. für Flash-, iOS- oder Linux-basierte Geräte oder PCs, wodurch aufwendigere Modelle mit individueller Authentifizierung jedes Betrachters zum Contentschutz und zur Videomonetarisierung unterstützt werden.



Mit der erweiterten DRM können Publisher Videos flexibler anbieten, mit Möglichkeiten wie Verleih, Abonnements für Video-On-Demand (SVOD) und Paketen mit mehreren Videos. Zudem können Regeln für den Zeitraum festgelegt werden, in dem die Videos abgespielt werden dürfen. Erweiterte DRM kann zudem verhindern, dass ein Video über bestimmte Ports ausgegeben wird und festlegen, dass es mit bestimmten Geräte-IDs verknüpft wird, sodass die Benutzer es nur auf einer begrenzten Anzahl an Geräten abspielen können.

### Wie funktioniert DRM bei der Wiedergabe?

Geschützter Content muss vor der Wiedergabe für einen Betrachter entschlüsselt werden. Für die Wiedergabe muss der Content, genauer gesagt der Player für diesen Content, mit dem DRM-System kommunizieren. Im Falle von Flash Access kann der Player nahtlos mit zentralisierten Flash Access-Servern kommunizieren. Bei anderen DRM-Systemen muss der Betrachter eine kompatible DRM-Software auf dem Gerät installieren bzw. bereits installiert haben. In beiden Fällen kommuniziert die DRM-Software mit dem zentralen System, das die Contentlizenzen verwaltet und die Contentwiedergabe zulässt oder verhindert. Bei Flash Access benötigt der Betrachter abgesehen von Adobe Flash keine weitere Software.

## Was muss ich tun, um DRM für meinen Videocontent zu implementieren?

### Wie erhalte ich DRM?

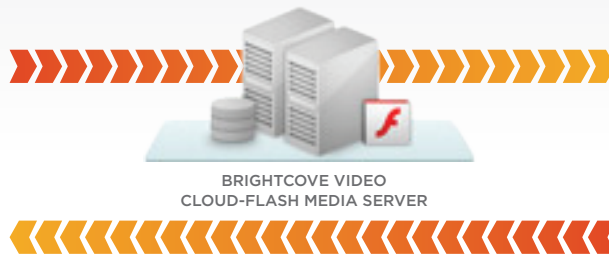
Im Bereich DRM gibt es Dutzende Unternehmen und eine Vielzahl an anonymen und erweiterten DRM-Systemen, die für unterschiedliche geschäftliche Anforderungen zur Verfügung stehen. Möglicherweise sind für die Unterstützung auf verschiedenen Wiedergabegeräten wie Mobiltelefonen, Tablet-Computern und internetfähigen Fernsehern unterschiedliche DRM-Systeme erforderlich. DRM-Technologien sind meist bei Softwareunternehmen wie Adobe oder bei Diensteanbietern wie Brightcove verfügbar. Damit DRM als Dienst bereitgestellt werden kann, muss der Anbieter strenge Sicherheitsstandards beachten. Diese betreffen das für das DRM-System verantwortliche Personal, die physikalische Umgebung des Systems sowie die Hard- und Softwarekonfigurationen. Ein Contentanbieter kann DRM-Software auch selbst kaufen und die Bereitstellung von sicherem Content selbst übernehmen. Aktuell bietet Brightcove eine auf Adobe Flash Access basierende DRM-Lösung an.

## Welche Optionen stehen mir beim Contentschutz zur Verfügung?

Welches DRM-System für Ihren geschäftliche Bedarf geeignet ist, hängt von Ihren Contentanforderungen, Ihrem Budget und den Geräteanforderungen ab. Hinzu kommt, dass dieser Markt sehr dynamisch ist. Die Voraussetzungen für einige Plattformen ändern sich mindestens einmal pro Jahr. So stehen möglicherweise zahlreiche Optionen bei der Ausrichtung auf eine Plattform für internetfähige Fernseher zur Verfügung, bei Android- oder iOS-Geräten sind diese Optionen allerdings eingeschränkter. Nach Auswahl eines geeigneten DRM-Systems müssen Sie überlegen, wie Sie den Content packen. Der Contenteigentümer kann den Content packen und verschlüsseln, bevor er einem Dienstanbieter wie Brightcove oder einem Content Delivery Network (CDN) bereitgestellt wird. Alternativ kann der Dienstanbieter das Packen übernehmen.



BRIGHTCOVE VIDEO  
CLOUD-PLAYER



**ADOBE FAXS**  
Flash Access DRM-Dienste

## Fazit

Obwohl einige noch immer glauben, dass DRM nur große Medienunternehmen und Contentproduzenten betrifft, spielt DRM in der Realität eine wichtige Rolle bei Onlinevideoinitiativen jeglicher Art. Wenn Sie Ihren Content schützen und seine Nutzung kontrollieren, können Sie gewährleisten, dass Ihre Onlinevideostrategie den von Ihnen gewünschten Zweck erfüllt und dass dieser nicht durch nicht autorisierte Aktivitäten beeinträchtigt wird.