

# User and Content Security: Qumu Video Engagement Platform

How Qumu protects both users and content with end-to-end encryption, viewer monitoring and content controls

## USER AND CONTENT SECURITY AT A GLANCE:

- Encryption Single Sign On
- Advanced Password Settings
- IP Restrictions OAuth Tokens
- Retention Policies Access Control
- Role-Based Permissions Author/Content Management
- Audit Trails



**GDPR Compliant**

## Our Approach

Organizations of all sizes and in all verticals rely on Qumu Video Engagement Platform to securely deliver the best possible video experience at scale, for both internal and external audiences. Qumu takes a holistic approach to user and content security—one that spans video encryption, Single Sign On, advanced user security, retention policies, audit trails and more. Qumu is the only choice for industries that value security the most: Banking, Financial Services, Health Care, Life Sciences, Manufacturing, Professional Services, Technology and Telecommunications.

## Security Audits and Controls

Qumu’s security vision is formed around a multi-layered strategy, which provides controls for content creation, data storage, video access and transfer. This strategy both includes and incorporates the following:

- Corporate security policies
- Personnel security
- Physical and environmental security
- Access control
- Systems development and maintenance
- Disaster recovery and business continuity
- Regulatory compliance
- Independent, 3rd party service penetration testing (PEN Test)



Data and Application Protection



Identity and User Controls



Viewer Tracking, Live Monitoring and Audit Controls

# A Holistic Approach to Security

## Encryption

Automatic protection and encryption of both internal and external video streams.

## OAuth Tokens

Only play content from web portals where users are already authenticated.

## User Authentication and Single Sign On

Control specific users and groups, and self-service configure SSO thru SAML 2.0 providers.

## Advanced User Security

Set password policies and enforce them across the environment, including expiration rules, timeouts, password complexity, user name and history restrictions.

## Retention Policies

Define content retention by group or by individual asset, with automatic content expiration, deletion and ability to archive.

## IP Restriction

Identify and control users of internal or external content, and apply custom rules at an individual content or group level.

## Content Classification & Approval

Define and enforce different content workflows and classifications for content and groups.

## Global Content Management

Leverage group-based functional controls and content and user audit trails, with either centralized or regional administration.



**4.7 out of 5**  
Security Rating

Enterprise-grade security for live streaming or on demand video content

### Learn more about:

Qumu Privacy Policy, Qumu Backup Policy, Qumu Disaster Recovery Procedures at [www.qumu.com](http://www.qumu.com)

Ready to get started? Our team is ready to help. Contact us at [info@qumu.com](mailto:info@qumu.com)



Qumu empowers hyper-distributed organizations to leverage the full power of video to move forward faster. Only Qumu's Video Engagement platform helps businesses build connectedness and shape a culture that is more engaged, motivated, aligned – and human – to drive impact in a work from wherever, whenever world.