VitalSource

Content Security

Content piracy and the commercialization of stolen or scraped content is a leading concern in higher education, especially as the shift to digital expands. Whether it is bad actors seeking to steal and commercialize stolen content, or unauthorized sharing and usage of material, these practices put publishers' intellectual property, revenue, and reputation at risk.

Protecting your content is our top concern at VitalSource, and we take exceptional measures to ensure the security of our platforms and your content.

OUR PLEDGE

We have an ongoing commitment to:

- Securely deliver millions of titles each year
- Conform to global security and compliance standards
- Provide exemplary digital rights management protections
- Evolve our strategies to protect against new and emerging threats
- Test our security measures through external validation

At VitalSource, our broad range of content security measures provides protection throughout the content workflow, from the time source files are delivered to our platform to the moment secured content is delivered to and in use by learners.

DELIVERING CONTENT

To protect your content from being lost or vulnerable during the transfer process, VitalSource has a clearly defined secure delivery and transport mechanism; unique credentials for each user; and delivery systems that are routinely scanned and audited for vulnerabilities.

STORING CONTENT

Content that is not properly protected during storage can be vulnerable to breaches. VitalSource securely stores all content at rest and during transit using AES256 encryption. We restrict access to content to a limited number of people internally with this list being audited routinely. Content that is no longer needed for distribution is routinely and safely purged. In addition to these standards, we employ secure logging and auditing of internal access to content.

DIGITAL RIGHTS MANAGEMENT

Digital rights management (DRM) is a critical part of the content fulfillment workflow; without strong protections, intellectual property and revenue can be at risk. VitalSource's partners establish the parameters for licensing and distributing their content; our DRM enforces their decisions and protects their content. We provide the best security options with industry-leading encryption, countermeasures, and technologies.

Encryption: We provide encryption while content is moving between any two devices or platforms. Data is encrypted and secured in motion and at rest.Only encrypted content is distributed externally, and it is only able to be read while the application is in use. Each asset is encrypted with a key that is unique to the asset and the user's device.

Countermeasures: Our advanced countermeasures for defeating scripts and scraping applications include high-definition device fingerprints and behavioral analysis powered by machine learning. Additionally, we have rooted devices and debuggers, and compile time obfuscation and key hardening. Online access is restricted to one concurrent login, and downloads are restricted to a preset number of devices per active license.

Best-in-Class Technologies: We recognize that the sophistication of bad actors will always be increasing. VitalSource utilizes the most advanced tools available to wrap and harden our already industry-leading security measures. These are the same best-in-class technologies being employed by leading vendors in the media industry and include Payment Card Industry Data Security Standard (PCI DSS) Support; two-factor authentication for administrative access; RSA public/private key; CloudFlare; Cloud Armor; and DRM hardening technologies.

MONITORING & ALERTS

VitalSource utilizes active monitoring and alerting for intrusion and piracy attempts, as well as monitoring of well-known internet locations where content piracy is discussed. Our user and system thresholds are set to alert on improper activity, and our staff is on call and able to respond to security alerts and issues 24/7. These measures allow us to quickly identify new threats as they emerge and minimize exposure.

EXTERNAL VALIDATION

VitalSource employs routine external validation to identify gaps in our technology's security. Our external validations include intrusion and penetration testing, and regular inspections and audits of DRM and licensing models. Our third-party systems are hosted in data centers certified as ISO 27001 and PCI DSS Service Provider Level 1. These external systems and services undergo thorough third-party technical and contractual due diligence. VitalSource has also obtained SOC II Certification.

CERTIFICATIONS

SOC II
ALCPA/SOC
GDPR
Data Protection Act 2018
FERPA
Digicert
California Consumer Privacy Act
PCI DSS
COPPA Compliant
IMS Global

CONCLUSION

Your content is your business. Protecting it is ours. With our continued commitment to utilize the best available security measures, you can depend on VitalSource to help you expand the reach of your digital content safely.