FORTRA

The Media And Entertainment Guide To Protecting Pre-Release Content

Content is your business, and that content is on the movie

In media, more than any other industry, content literally is the lifeblood of business. And for the business to thrive, that content must be able to flow. An extended web of production teams needs to collaborate on audio and video files. Scripts need to be edited, reworked, and shared with agents and talent. Strategies, production plans, and deadlines also often adapt. And throughout this process, production partners, talent agencies, and competitors are all trying access this content.

However, sharing content today is the easy part. Keeping it safe is another story. Organizations and individuals have thousands of vectors for moving your content, intellectual property, and financial information —email, Dropbox/Box shared links, managed and unmanaged mobile devices, Slack, or even a good ole' fashioned USB drive. And all it takes is one rogue or momentarily distracted user for your content to be exposed to the world. This reality requires a new approach to security.

WE'LL CUT TO THE CHASE

In media and entertainment, content is king. To protect that content, you need a security model that puts the data first so that your content remains secure no matter where it goes, how it gets there, or who handles it. At Vera, that's what we do.

DLP, CASB, DRM and Classification tools aren't enough "what's a Data-Centric strategy?"

Data Loss Prevention, Cloud Access Security Brokers, Digital Rights Management and Classification tools offer their own valuable benefits, but they all share the same limitation: They're all about controlling initial access. But what happens after that access? Once confidential content leaves your network and is downloaded by an employee or a production partner, your security strategy comes to an end. As your IP travels to unknown endpoints, unknown agencies, and unknown domains, all bets are off. You can't see it. You can't control it.

A recent study Gartner estimates that 75% of organizations implementing data classification policies have limited deployments and see no tangible benefits and that, only 1 in every 10 businesses with integrated DLP have a well-defined data security governance program in place.

In a nutshell, having only these tools isn't enough.

GARTNER STUDY

These tools rarely work at the most critical moment—when people are working with the information.They can't prevent a talent agency from saving a copy of your script and forwarding to another client, who then passes it on. They can't secure information "in use." And once your data moves past the DLP fence and CASB proxy, it's in the wild and unprotected.

Digital Rights Management (DRM)

An attempt at data-centric security but a cumbersome user experience prevents enterprise-wide adoption and scalability.

Cloud Access Security Broker (CASB)

Enforce security policies and block information leaving cloud applications (e.g., Box, Dropbox) but once data is downloaded or moved offline, security teams lose all control of what happens next.

Data Loss Prevention (DLP)

Scans and quarantines confidential information traversing the network but once it leaves, security teams can't see, audit or control what others are doing with mission critical data.

Classification

Tags and classifies sensitive information shared from your business but a classifier won't be able to prevent an internal employee from downloading trade secrets and taking them to his/her next job.

Data-Centric Security: Security for the porous organization

Data-centric security is the ability to secure data through its entire lifecycle, everywhere it travels, no matter who has it or where it's stored. The goal is to protect confidential data at the point of its greatest vulnerability—when it's being used in others' hands, and as it travels outside our perimeters into unmanaged domains, devices, and applications.

The Media & Entertainment Script For Data-Centric Security That Protects Your Content And IP

How does this work in media and entertainment?

Security teams for media organizations are often balancing between two competing demands: securing intellectual property from pre-release leaks while enabling collaboration and production.

Your security team is naturally laser focused on protecting your unique content and IP—audio/video files, scripts, casting information, game designs, production schedules and budgets, etc. But to achieve a final cut, the business must share highly confidential information with industry contractors, partners, and employees who may not necessarily be with your company forever.

Data-centric security solves that balancing act. Even more, it provides the solution to the questions keeping your team up at night:

How do I control how production partners consume our pre-release content?

Revoke access or adjust permissions for files, anywhere

How do I prevent leaks to unauthorized partners or competitors once an employee or partner has access to our scripts or content?

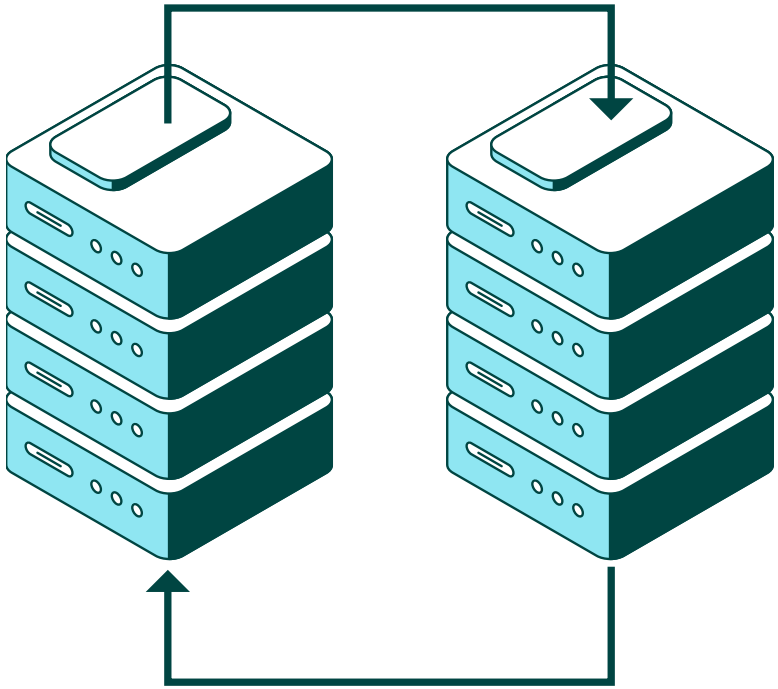
How do I audit our data throughout the production lifecycle?

How can a share sensitive planning, casting, and bud geting emails while ensuring they can’t be forwarded to a 3rd party?

How do I revoke access to proprietary information once an employee leaves the company?

The media and entertainment script

At Vera, we've helped a wide variety of media organizations protect their content. In the course of this work, we have seen a script emerge on how media security teams are leveraging data-centric security to automate their job and become a value-driven enabler to the core business.



Automatically secure pre-production plans to third-party partners

Even before we get to securing media content, it's critical for organizations to have tight control over email (e.g., Microsoft Outlook, Apple Mail, etc.). Planning, budgeting, casting information, and scripts will all naturally flow through email. Leveraging Vera's smart rules engine, all attachments sent to a partner (example: @acmetalent.com) are automatically secured without requiring your employees to take any manual steps to secure data.

If data is ever forwarded to a party that doesn't belong to the AcmeTalent domain, that third-party will never be able to access your company's crown jewels.

Prevent leaks, even after content is downloaded from your collaboration systems

Media teams use local file shares, Box, Dropbox, SharePoint, OneDrive, and other cloud storage platforms to store, share, and collaborate on a wide variety of large pre and post-production media files.

Vera has built out-of-the-box integrations to all of these storage systems to automatically secure any file uploaded or downloaded from those platforms. That way, your employees and partners work exactly the way they normally would, and Vera works seamlessly behind the scenes to protect your IP— everywhere it moves.

Vera's security sticks to the file anywhere it goes, making sure only authorized parties are working with your content. Content can be shared with specific individuals, groups, or organizations, and access can be pulled back at any time even after it has been shared.

Audit and track content throughout the production ecosystem

With Vera, media companies can monitor and audit all of their third-party partners to understand exactly who is consuming content, track all access attempts (authorized or not), and get granular metrics on usage. In the past, more recipients meant more exposure and vastly higher chances of a leak, and in many cases organizations could only watermark their content and hope for the best. With Vera, organizations can share and collaborate with countless third parties while retaining full control and accountability over the content, with a complete audit trail of all access.

Revoke access to data when a job is complete or employee leaves

Production projects can span many months and many partner organizations, and employees are constantly moving on to new roles in organizations.

Vera's Dynamic Data Protection allows media companies to revoke access to data at any time even if it's been moved to a personal account. This means that once a partner's job is done, their access to that content can be pulled back to limit the exposure of the data even if it has been copied. If an employee leaves the organization, their access to the data and all copies are likewise removed. In one click, security teams can rescind access to an individual, a team, or an entire organization to retain control over their IP, in real-time

Secure content generated from home-grown or specialty apps

Media organizations often have their own tools and processes, and security can't afford to slow down valid work. The Vera SDK/API allows security teams to integrate data security into their home-grown and custom apps.

With the Vera SDK, production files, game designs, and art can be uploaded and shared from home-grown systems or third-party apps and automatically secured—giving you a powerful data security fabric for your entire ecosystem and extended enterprise.

Interested in learning more about data-centric security? Let’s discuss how Vera can help you.

Visit us at www.vera.com/contact-us to get in touch.

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-vr-gd-1222-r1-79d