am audible magic®

Automate Management & Administration of Your Network Use Policies

Benefits:

- Leverage user-focused "teachable moments"
- Save time, staffing and money
- Up and running in minutes with minimal maintenance
- Integrate with your judicial systems

Features:

- Detect illegal sharing of copyright compliant via P2P networks
- Plug-n-Play configuration
- Automate student communication
- Zero false positives for copyright identification
- 1GB and 10GB NIC Support
- HEOA Compliant
- Pass-by mode of operation
- Highly scalable

Audible Magic Corporation
985 University Ave. Suite 35
Los Gatos, CA 95032, USA

telephone: +1.408.399.6405
fax: +1.408.399.6406
www.audiblemagic.com

The Audible Magic Solution

The CopySense® Appliance helps campus IT networks reduce DMCA-infringing sharing of copyrighted media content on peer-to peer (P2P) networks. It balances an educational institution's desire to offer unfettered access for non-infringing P2P traffic against the need to educate good digital citizenship and reduce IT workload related to DMCA takedown notices.

The appliance uses Audible Magic's patented content recognition technology to accurately identify public transfers of commercially registered audio or video files. The flexibility of Audible Magic's technology enables a university to match product capabilities with their own unique set of network use policies and disciplinary actions.

The CopySense Appliance also allows educational institutions to remain compliant with the Higher Education Opportunity Act (HEOA) of 2008, which requires compliance with and control/education of any students involved with the illegal sharing of commercially registered, copyrighted content.

Graduated Response Leverages the Teachable Moment

Research has shown that the most effective long-term method for controlling inappropriate Internet use is through education. The CopySense Appliance includes Audible Magic's unique Graduated Response system, which is an automated way to educate users on network policies, saving you save time, staffing and expense. At the time of an infraction, Graduated Response immediately and automatically responds with messaging to the user. With your users' attention focused on the just attempted event, you take full advantage of the *teachable moment*. The result is a new generation of educated and law-abiding digital citizens and a subsequent reduction in DMCA takedown notices. Graduated Response is fully customizable so you can communicate specific campus network use policies, provide information on the appropriate use of copyrighted intellectual property and/or apply appropriate sanctions.

How It Works

The CopySense® Appliance functions as a passive network device that works in a "pass-by" mode, monitoring mirrored traffic from your firewall. It extracts and performs analysis on publicly shared P2P traffic to compare characteristic "fingerprints" of audio and video content against a database of commercially registered media content. Any content not matching these fingerprints is ignored. A match indicates copyrighted material that is being shared illegally. Using this information and the context of the violation (1st infraction, 2nd infraction, etc.) the CopySense Appliance invokes a TCP redirect to focus user attention to an educational page warning them of their action and requiring them to read about and accept campus policy. Using Graduated Response, the appliance is able to respond to repeat offenders by raising the sanction level including stopping network access unless the user speaks to Student Services.
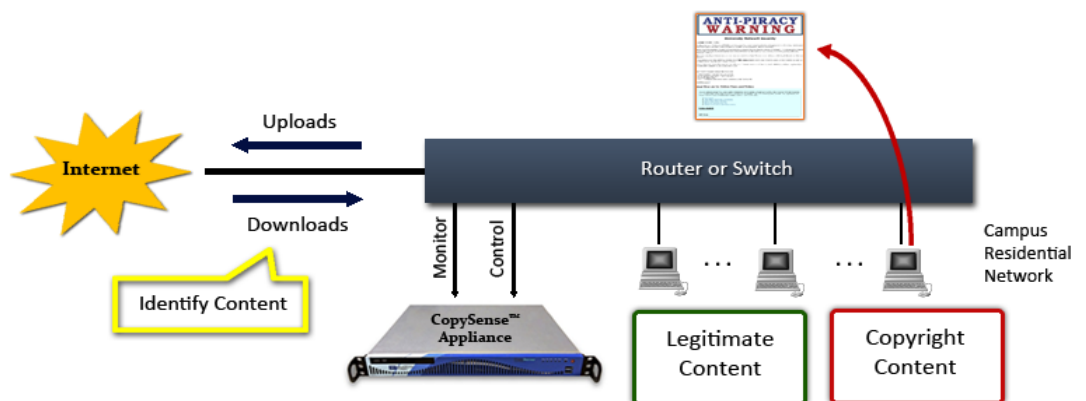
Detect Violations of Your Network Policy

To match each institution's unique network policies, the CopySense Appliance offers a number of easily configured options to detect various infringing activities.

Copyright Identification

The patent-protected copyright identification of music and video accurately identifies transfers of registered content over peer-to-peer networks. Identification is done with zero false positives, which means legitimate traffic is not affected. Audible Magic maintains one of the largest databases of registered content with the media industry registering new music, film, TV and other content daily. The technology is flexible in recognizing content using various file formats and is resilient to compression methods.

Peer-to-Peer File Sharing Activity

File sharing of copyright material is most frequently conducted over peer-to-peer networks. The appliance detects and manages this activity by user.

Bayesian Filtering

Similar to spam-filtering software, Bayesian filtering is used by the appliance to detect highly probable transfers of copyrighted and/or other inappropriate content. This is an optional filter that can be enabled to catch probable matches.

White/Black Listing and Keyword Identification

Keyword identification enables an institution to customize detection of other activities such as the inappropriate file sharing of digital textbooks and other academic works. Allow/Restrict access by user, IP address ranges and/or keyword phrases in metadata.

Features

Easy Installation, Setup and Management

The CopySense® Appliance comes pre-configured as a 1-U rack-mountable system. Simply connect to your network via two LAN connections – one to passively listen to network traffic via a mirror port and the other to provide control information back to the network. All functions are managed via an easy-to-use web browser interface. You can choose to manage the entire network or specific subnets.

Easy Report Generation

A variety of report formats have been designed to inform you about file sharing activity on your network. These reports show P2P bandwidth utilization versus your total bandwidth over time, number of infringing transfers over time, and more detailed reports containing a list of copyrighted files uploaded from or downloaded to your network. Report export format options are csv, xml, or html.

Automate management and administration of campus network usage policies

The CopySense Appliance automates the management and administration of your campus wide network usage policies by communicating and educating users who violate these policies by sharing content illegally via peer-to-peer networks. No additional steps have to be taken by Campus IT staff or network administrators unless a sanction is issued or a user continues to violate campus policies.

Integration with your Radius and DHCP Servers

By integrating with your Radius and DHCP servers, the CopySense Appliance is able to identify users and continue managing them through the different Graduated Response levels that increase in severity with every continued infraction. Only when the users hit the highest tier do Campus IT or Student Services need be involved.

Customize rules to identify illegal sharing of confidential material

Network administrators can add additional rules to either capture additional transfers or to allow for the unsanctioned sharing of certain types of content. This is done in accordance with campus network policies to suit every university's unique needs.

Automatic Signature Updates via a subscription service

The AutoUpdate Subscription Service provides each CopySense Appliance with daily downloaded updates including newly registered copyright information and new detection methods to tackle countermeasures from third parties. This is similar to how antivirus and antispam software keep current with the latest detection methods

No Impact on Your Network Performance

Detecting inappropriate uses and violations of your network policies does not affect legitimate network traffic The CopySense Appliance introduces no points of failure to your network and does not introduce any latency, jitter or packet-loss.