Cybersecurity for Media Production and IT Environments

IP Unlocks Greater Business Opportunities
Network transformation from SDI to IP is enabling greater agility, less cost, and flexibility to deliver premium 4K/UHD content across virtually any device at any time, anywhere. Within the production environment, this content can be generated at a rapid rate. Video can be shot, produced, edited, and distributed by creative artists linked through powerful networks across multiple studios. Production companies are in a unique position to take advantage of these new trends with cloud and over-the-top (OTT) technologies.

New Threats Are Affecting the Media Business
The rapid rise of cloud and IP is creating new business opportunities to monetize premium content, but linking digital media production and delivery across an IP network presents myriad security challenges. Your valuable video content and your subscribers’ personal data are stored together inside your media data centers which are becoming increasingly vulnerable to sophisticated hackers looking to harm your business and make a profit.

Criminals can use attacks that are faster, stealthier, and more dangerous than ever to break into the media production and delivery environment to:
- Leak, steal, or ransom premium video content
- Replace or modify content in the data center to affect your live broadcast
- Alter security settings and access rights to compromise conditional access and Digital Rights Management (DRM) systems
- Use denial-of-service or other targeted attacks to disrupt your subscribers’ experience and prevent you from distributing content and running your business
- Compromise customer relations management (CRM) and billing systems in your data center to steal customer information (SSNs, credit card numbers, user names, passwords, access credentials, and so on), damaging your business and your reputation in the industry

Comprehensive Media Infrastructure Security
Media-production networks, corporate IT, media-storage locations, and customer data need to be access controlled and defended against intrusion. Yet those measures should not inhibit the creative process or other activities to run the business. To mitigate threats, you need to block access to potentially malicious webpages or email that could be vehicles for attacks. It is not enough to defend the network perimeter. Your security solution must continuously monitor the entire IT environment in case unknown threats get in. Only then can you quickly detect, contain, remediate, and respond to breaches before they damage your business.
Cisco’s approach to media production and IT security:

- Protects premium content and customer data with the most comprehensive protection across the entire media production and content delivery value chain, from creation through consumption
- Provides granular access control over, as well as enhanced visibility into, everyone and every device on your network
- Locks down the corporate network and the media infrastructure to stop threats before they can cause damage and quickly remediate if they do manage to get in

With Cisco, your media production and corporate IT environment is protected by the world leader in cybersecurity. We achieve this with a robust approach to deliver effective security that enables you to see more, protect better, and respond more quickly against cyberattacks.

**Cisco Cybersecurity for Media: How It Works**

Our multilayered cybersecurity solutions include next-generation firewalls (NGFWs), next-generation IPS (NGIPS), distributed denial-of-service (DDoS) mitigation, advanced malware protection (AMP), policy and access, network visibility and enforcement, cloud security, web security, and email security.

Cisco Firepower® NGFWs use granular access control and identity checks to strengthen your network perimeter and lock your media production data centers and corporate IT before an attack happens:

- See and control all video production and corporate traffic
- Eliminate unauthorized access of video content and customer data
- Quickly segment users and grant access based on category or role

If an attacker tries to compromise your business through the network, web, email, and/or DNS, our integrated Cisco Firepower NGIPS, DDoS, cloud security delivered by Cisco® Umbrella, and web and email security solutions protect against the threats as they happen:

- Protect network and critical infrastructure from advanced threats
- Prevent service disruption from application DDoS attacks
- Keep your web, email, and DNS safe from spam, malware, and other threats with continuous protection
If malware does manage to get in, network visibility and enforcement by Cisco Stealthwatch®, along with Cisco AMP and Cisco Threat Grid sandboxing solutions (on premises or in the cloud), continuously scan traffic and files to find threats before they become active. If malware does become active, we can isolate the threat and remediate the infection or bring you back online quickly by using Cisco Identity Services Engine (ISE) together with Cisco Firepower and/or Stealthwatch solutions:

- Protect against hidden malware or targeted attacks
- Address new attacks and malware with real-time file analysis
- Remediate quickly after an attack by tracking file trajectory in the network and determine a remediation plan

Cisco Security Architecture for Media enables robust security solutions to provide protection across your media infrastructure and corporate IT systems.

Cisco Security Services are also available to help you design, implement, and manage your security each step of the way so you have the best protection across your business.

**Helpful Links**
- [Service Provider Security](#)
- [Cisco Security for Video](#)