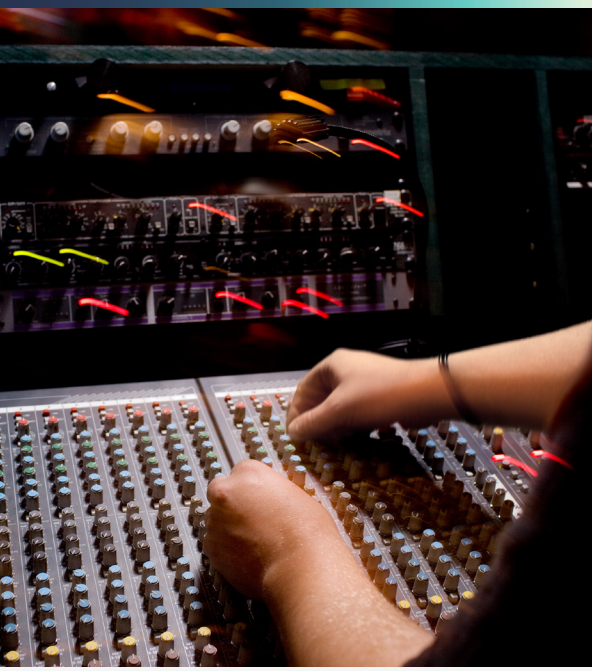
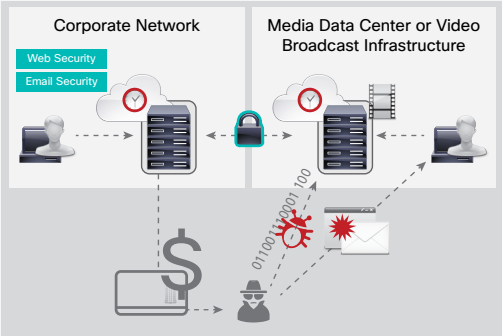
At-a-Glance



Our number one data center security solution protects your business, services, customer data, and media content

- See and control all video and corporate traffic
- Eliminate unauthorized access of video content and customer data
- Quickly and easily segment users and grant access based on category or role
- Discover hidden threats and potential thefts of video content and data



Threat-Centric Security for Media Production and Broadcast

Growing Business Opportunities, New Threats

It is an exciting time in the broadcast media industry. Film production is growing at a rapid rate. Video can be shot, produced, edited, and delivered by creative artists linked through powerful networks across multiple studios. And production companies are able to take advantage of cloud and over-the-top (OTT) technologies to deliver content directly to viewers on virtually any device. The business opportunities to monetize video content are boundless, but linking film production with the business of entertainment delivery presents myriad security challenges. Video content and your viewers' personal data are now stored together inside your media data centers. They are both more vulnerable to hackers.

Criminals can use attacks that are faster, stealthier, and more dangerous than ever to break into the video 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, etc.), 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, and remediate breaches before they damage your business.

Only Cisco delivers the comprehensive security solution to safeguard your media assets and critical business data from creation to consumption

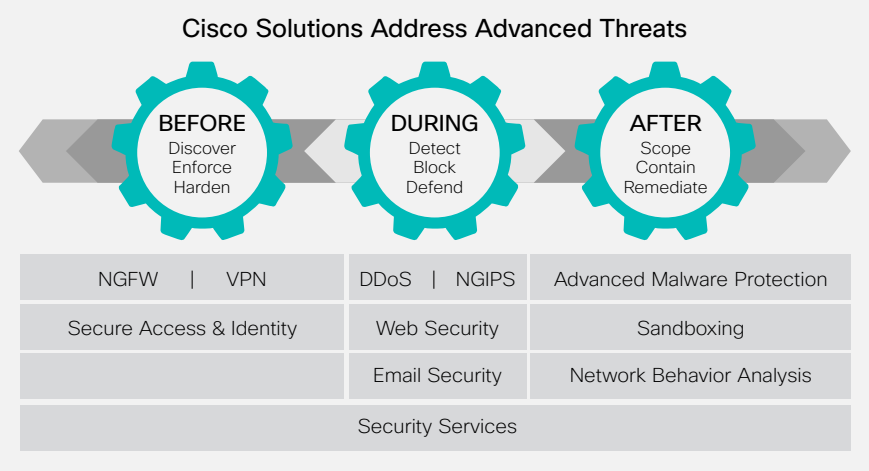
Cisco's approach to media data center and IT security protects content and customer data when they are created, distributed, and consumed. You get granular access control over, as well as enhanced visibility into, everyone and every device on your network. You can lock down the corporate network and the media infrastructure to stop threats before they can cause damage and quickly remediate if they do manage to get in.

Cisco Protects Your Video Production Infrastructure

With Cisco, your media data center and video headend are protected by the number one solution in data center security and the largest threat telemetry network and research team in the world. Our multilayered solution works to ensure that your content, services, and business are protected from advanced threats across the attack continuum: **before**, **during**, and **after** an attack.

Before: Our next-generation firewalls 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



During: If an attacker tries to compromise your business through the network, web, or email, our integrated next-generation intrusion prevention system (NGIPS), distributed denial-of-service (DDoS), 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 email safe from spam, malware, and other threats with continuous protection before, during, and after an attack

After: If malware does manage to get in, network behavioral analysis by Cisco® Stealthwatch, along with Cisco Advanced Malware Protection (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.

- 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 brings a wealth of robust security solutions to provide comprehensive 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.

Next Steps

Contact your Cisco sales representative for more information.

Find out more at Cisco Secure Data Center Solution.

C45-737721-00 08/16