At-a-Glance

Data Center Security for Video Services

Our number one Data Center Security solution protects your content, services, and customer data

Secure your business

- Protect video content and customer data from cyber attacks to your video headend and data centers before, during, and after an attack.
- Protect service and content distribution over any network to any device.

Cisco's comprehensive approach to security for video service providers adapts to a changing threat landscape to protect your business, services, and content

New Opportunities, New Threats

The video industry is undergoing a massive transformation driven by the growth of cloud and over-the-top (OTT) delivery. You are upgrading your infrastructure to rapidly deliver content on demand through open IP networks, regardless of device or connection method. Unfortunately, this makes securing content more difficult. And as video content and customer data are increasingly stored inside your data centers, they are more exposed to attacks. Criminals can use attacks that are faster, stealthier, and more dangerous than ever to break into the video headend to:

- Leak or steal premium content
- Replace or modify content in the data center to affect live broadcasts
- Alter security settings and access rights to compromise conditional access (CA) and digital rights management (DRM) systems
- Use denial-of-service or other targeted attacks to impair your subscribers' experience and prevent you from distributing content and running your business
- Compromise customer relationship management (CRM) and billing systems in your data center to steal customer information (SSN, credit card numbers, user names, passwords, etc.), affecting your business and damaging your reputation in the industry

Threat-Centric Security for the Video Headend

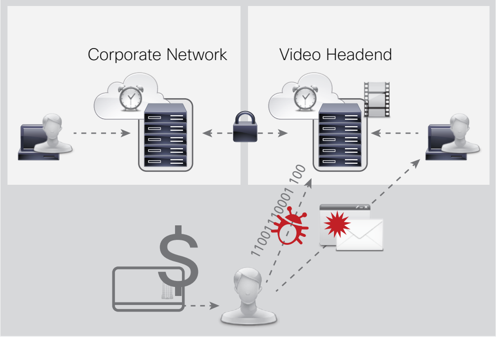
Cisco's approach to video data center security safeguards content and customer data from advanced threats when that content is created, distributed, and consumed. With granular access control, as well as enhanced visibility into everyone and every device on your network, you can lock down the video broadcast infrastructure to stop potential threats before they can cause damage, and you can quickly remediate if they do manage to get in.

See and control all video and corporate traffic

Eliminate unauthorized access of video content and customer data

Quickly segment users and grant access based on category or role

Discover hidden threats or potential video content or data thefts



Cisco Protects Your Video Delivery System

With Cisco, your video headend and data center are protected by the number one company 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 video headend and data centers before an attack happens.

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

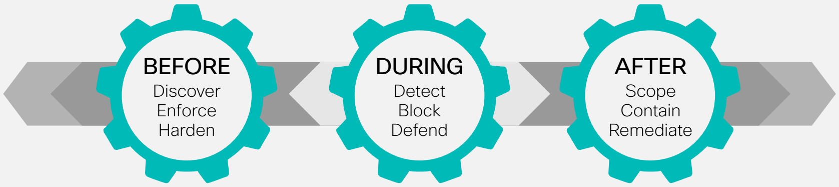
During: If an attacker tries to compromise your business through the network, the web, or email. Our integrated next-generation intrusion prevention system (NGIPS), distributed denial-of-service (DDoS) defense, and web and email security solutions protect against the threats as they happen.

- 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 and Cisco Advanced Malware Protection (AMP) and by Cisco Threat Grid sandboxing (on premises or in the cloud) continuously scans 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 Solutions Address Advanced Threats



BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

NGFW | VPN	DDoS | NGIPS	Advanced Malware Protection
Secure Access & Identity	Web Security	Sandboxing
	Email Security	Network Behavior Analysis
Security Services		

Cisco brings a wealth of robust security solutions to provide comprehensive protection across your headend 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 to ensure 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.