



Cisco Videoscape Control Suite Multi-Conditional Access and DRM Management

DISCONNECT CONTENT SECURITY FROM THE VIDEO CONTROL PLANE

What Is the Value of Cisco Videoscape Control Suite Multi-Conditional Access and DRM Management?

In the past, when you chose your cable system, you also chose your content security. That is because, in early systems, many of which are still operating today, conditional access has been inseparable from the video control plane.

But what does that mean, when you are creating new multiscreen services that can move from a set-top box (STB) to a mobile device and back again, within a single session? Until now, it has meant a complicated effort to manage different conditional access and digital rights management (DRM) systems, switching between completely separate control planes.

Cisco Videoscape™ Multi-Conditional Access and DRM Management decouples content security from the control plane. It treats content security as a cloud service that you can invoke and apply to content, wherever you need it. So for the first time, you can interface with multiple content security systems – encrypting content for older STBs, newer video hardware, and your subscriber's personal devices – from a single management console (Figure 1). As a result, content security just became a lot simpler and less expensive.

What Problems Does It Help Solve?

To successfully deliver current video services alongside new multiscreen experiences, you need to:

- Simplify the process of creating business rules for content-security applications
- Reduce the complexity and costs of managing multiple control-plane security systems
- Implement a more open architecture that can support new content-security systems alongside old ones
- Lower capital costs for encryption hardware in the STB and the headend

Figure 1. Unified Security Across All Devices



Cisco Videoscape Multi-Conditional Access and DRM Management

Cisco Videoscape Multi-Conditional Access and DRM Management re-imagines content security to make it easier and less expensive to manage. The solution is part of the Cisco Videoscape Control Suite (VCS), a comprehensive control-plane framework for modern, cloud-connected video systems.

This new approach to content security implements application logic for security functions like encryption and entitlement as cloud services, allowing them to be applied to multiple conditional access and DRM systems. Using open APIs, you can expose video content to conditional access, DRM encryption, and account-based entitlement control in the same way you would apply any other web service in the data center. So you can control multiple conditional access and DRM systems at the same time, from a single interface.



An Open Security Architecture

One of the key elements of the solution is Simulcrypt, an open and widely used content-security framework that quickly and easily accommodates multiple conditional access and DRM systems. We have redesigned our industry-leading Cisco® PowerKEY® conditional access architecture to be Simulcrypt compliant. So you can now control content security for your deployed Cisco PowerKEY STBs, as well as newer devices that use Cisco VideoGuard® Conditional Access and DRM from the same system.

In fact, because the solution uses an open architecture, you can now add any Simulcrypt-compliant encryption system to your environment and manage it exactly the same way. Legacy conditional access, new DRM systems, and third-party security solutions all become interchangeable modules in your toolkit, which you can take out and use as needed.

What Are the Benefits of Cisco Videoscape Multi-Conditional Access and DRM Management?

With this modern Cisco approach to content security, you can:

- Extend video content to new devices more quickly, easily, and at a lower cost
- Lower operational expenses by unifying security business rules for your heterogeneous environment
- Manage security for both managed STBs and unmanaged personal devices from the same system
- Scale content security in the cloud and easily apply the right security to your content, wherever and whenever you need it
- Make it easier to deliver new multiscreen experiences, such as pausing video on an STB and resuming on a tablet
- Eliminate the need (and costs) for proprietary cable-card hardware, even when delivering content to older deployed STBs
- Eliminate the need for proprietary quadrature amplitude modulation (QAM) hardware that supports a specific entitlement-control system

Why Cisco?

Managing content security has been a longstanding challenge, and it is only getting more complicated as you add new multiscreen video services. That's why we are embracing an open, cloud-based architecture for conditional access, DRM, and entitlement control. We are committed to making it as easy and inexpensive as possible for you to use whatever security systems you need, wherever you need them.

It is a big change to the way you manage content security. But with our broad portfolio and industry-leading expertise in both conditional access and DRM, including legacy and state-of-the-art systems, we can provide a complete, unified solution.

For More Information

To find out more about Cisco Videoscape Catalog Management and the Cisco Videoscape Control Suite, contact your local Cisco representative or visit <http://www.cisco.com/go/videoscape>.