PRIMER

# Protecting Video Companies from Enterprise to Content to Viewer

Akamai

> *They're inside. Inside the perimeter. They're in here. They're inside. They're inside!"*
>
> *– Bill Paxton as Private Hudson, "Aliens" (1986)*

## Plot Point 1: The Enterprise Under Attack

Video production is an inherently collaborative act, and as our industry has moved to file-based workflows, the number of "endpoints" that can access or touch an asset has grown. That means the number of potential chinks in your security armor has also grown.

Take freelancers and post-production houses as examples. They typically don't consider themselves targets and may not have the resources or expertise to practice proper security hygiene even if they did. That makes them ideal targets.

For example, the famous *Orange Is the New Black* hack from 2018 was the result of financially motivated attackers' ability to compromise a post-production house working on the new season of the hit Netflix show. They stole the mezzanine-quality files and held them for ransom.[1]

At a recent closed-door *Cybersecurity for Broadcasters* retreat in the United States for more than two dozen companies, among the top requests were securing remote access and vendor security.

Here are two tools that can help:

1. Enforce a strategy of least privilege by using a Zero Trust Network Access tool for employees and contractors who seek access to key resources
2. Detect and block malicious traffic that originates inside the network using a secure web gateway (SWG)

These Zero Trust approaches will reduce the likelihood that the thief can get inside the vault – and if they do, limit their ability to make it to the getaway car.

> *My dad was a petty thief. He said, 'Everyone steals. That's how it works. I steal, son. But I don't get caught.'"*
>
> *– Christian Slater as Mr. Robot, "Mr. Robot" (2015)*

## Plot Point 2: Video Under Attack

In 2013, the psychological horror-thriller TV series "Hannibal" was cancelled due to "poor ratings." The series, however, was ranked as the fifth-most illegally downloaded show that year. Its producer, Martha De Laurentiis, said that the cancellation of "Hannibal" had a lot to do with piracy.[2]

In June 2019, Qatari broadcaster BeIN Media Group announced it was laying off 300 employees due to declining revenue. The cause? BeIN claims that rival service beoutQ pirates its ultra-premium sports content.[3]

Media piracy has been a part of our landscape since the silent movie era. The move to streaming and the globalization of distribution simply make it easier and more profitable for the bad guys. Studies on the impact of piracy vary dramatically, but analysts consistently find that video piracy generates at least $1 billion a year for the pirates in the United States[4] and another €1 billion in Europe.[5]

Piracy is also a multifaceted ecosystem, with amateurs livestreaming to friends on social media, "information anarchists" ripping and sharing first-run content via release groups, financially motivated attackers running sophisticated video services, and yes — nations using piracy as part of their information warfare campaign.

It's a tough nut to crack. We at Akamai work with many of the world's biggest video media producers and distributors, and we've been collaborating on an approach we call Protect, Detect, and Enforce. In summary:

### Protect: Stop content and credentials from being stolen

- Protect against theft of video production and storage systems
- Protect against theft of viewer details to prevent re-streaming
- Protect against geo and rights infringements
- Protect against playback infringements

### Detect: Discover who is using files once they've been stolen

- Deep log inspection can give you a real-time picture of infringing activity
- Proxy detection can find users of VPN services
- Watermarking can identify and trace stolen files

### Enforce: Take down pirates who use your intellectual property

- Token access revocation can stop offending IP addresses from streaming
- Stream modification can replace the pirated stream with alternative content
- Proxy blocking can stop the detected user from using that proxy IP

> *Our whole world is sitting there on a computer. Your DMV records. Your social security. Your credit cards. Your medical records. It's all right there, just begging for someone to screw with. And you know what? They've done it to me, and you know what? They're gonna do it to you."*
>
> *– Sandra Bullock as Angela, "The Net" (1995)*

## The Crescendo: Viewers Under Attack

In 2019, a major new subscription service was launched in the United States to massive success. But within 24 hours, some new customers lit up social media complaining that their accounts had been locked out. In this case, the cause was not a data breach but a credential stuffing attack.

When over the top (OTT) services discover a viewer's account has been compromised, many respond by requiring the paying customer to do an account reset to prevent further theft. That safeguards the company's intellectual property but results in a poor customer experience.

Many of these attacks take the form of automated "account stuffing," and one defense that can reduce the need for account lockout and reset is to use a bot management tool. Good ones can proactively identify when an actual person logs in and can block bots that pretend to be that same person.

And since identity is one of the fundamental building blocks of the OTT revolution, enabling great viewer experience as well as more profitable subscription-based and ad-supported business models, it's critical to protect those identities.

## The Denouement: The Hero's Return

As video producers and distributors finish their journey toward a more secure ecosystem, they surely know the attackers are simply licking their wounds and preparing their next attack.

As a key partner for both video delivery and cloud security, Akamai is in a good position to be your sidekick. Take a look at how we can help protect your enterprise and your apps and APIs, how we can help you scope and fight the piracy challenge, and how our bot management solutions can reduce the attack of the clones.

See you in the sequel.

## REFERENCES


1) Netflix hacked, 10 new Orange Is the New Black episodes leaked
2) Did pirates kill 'Hannibal'? | The Hill
3) BeIN axes staff claiming profits hit by piracy
4) Sandvine White Paper – Video and Television Piracy: Ecosystem and Impact
5) EUIPO Reports: Nearly €1B in illegal 'IPTV' streaming in 2018; overall piracy down slightly



Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 06/20.