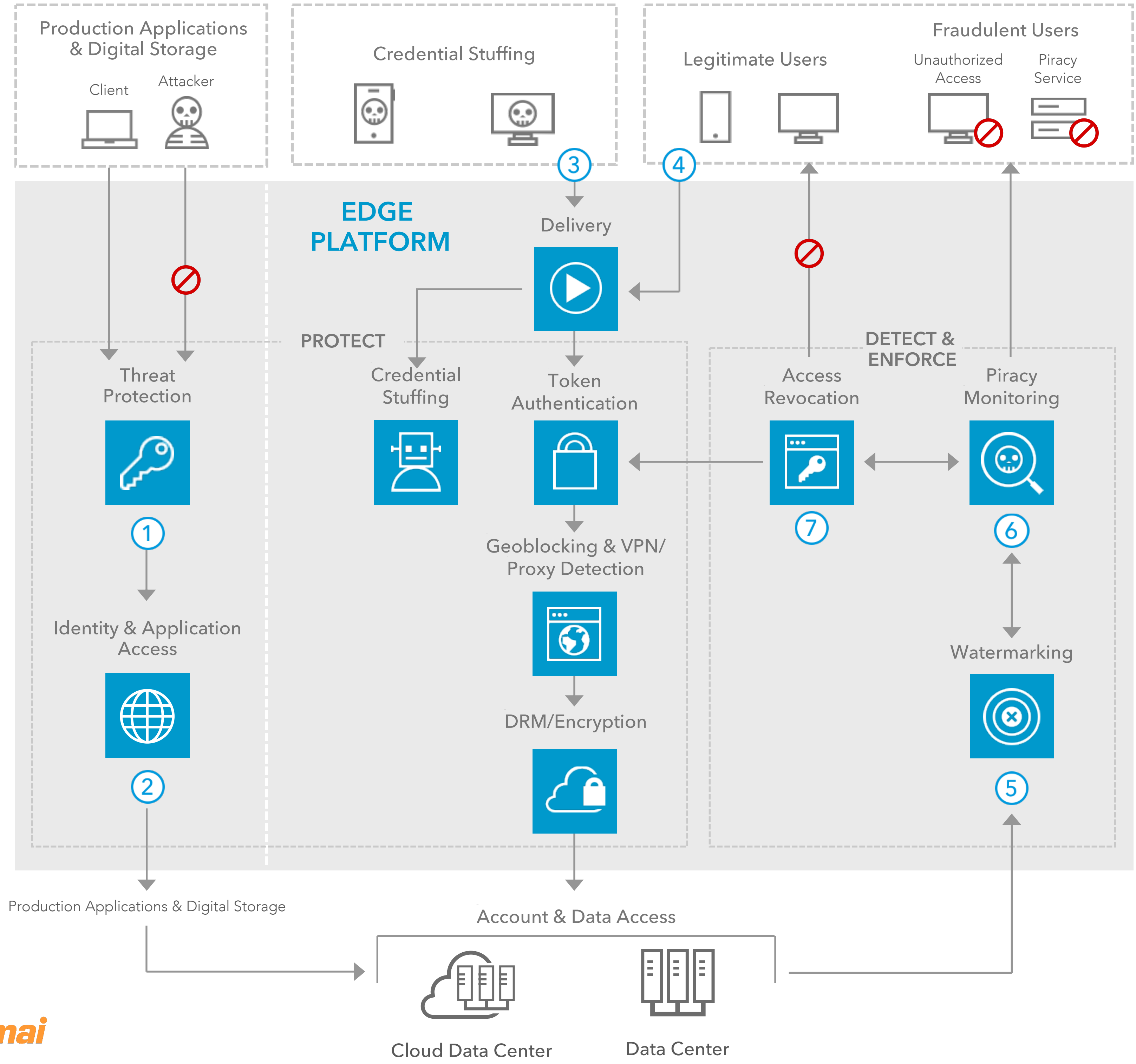
VIDEO PIRACY

Reference Architecture



Akamai

OVERVIEW

Video piracy poses a major threat to the media industry, impacting revenue, job opportunities, and licensing models. Businesses that create, manage, and distribute sport, TV, and movies online are subject to a range of attacks used by pirates to retrieve and distribute content, and should therefore consider solutions that secure their entire technical workflow. Akamai applies a 360-degree posture based on three core principles — protect, detect, and enforce — to help organizations mitigate the impact of video piracy.

1 Threat protection tools defend teams from phishing and man-in-the-middle attacks by pirates looking to infiltrate production or digital storage systems to steal content directly.

2 Based on identity and other security criteria, access to production and archive systems is granted to team members based on job function and permissions.

3 Protect OTT login pages by detecting and mitigating attempts to acquire viewer/subscriber details through credential stuffing.

4 Grant access to video streams for legitimate viewers who have a valid token. Prevent access to viewers coming from known VPN or proxy services or a geo-restricted area. Apply encryption or DRM to prevent distribution to unauthorized viewers or devices.

5 Actions by fraudulent viewers are traced using forensic watermarks applied to content.

6 Piracy monitoring services discover sources of leaked content and act against fraudulent activity.

7 Fraudulent users streaming or sharing content illegally have their access revoked in near-real time.

KEY PRODUCTS

Threat Protection ▶ Enterprise Threat Protector

Identity and Application Access ▶ Enterprise Application Access, Kona Site Defender

Credential Abuse ▶ Bot Manager Premier, Kona Site Defender

Content Protection ▶ Adaptive Media Delivery: Media Encryption, Enhanced Proxy Detection, Access Revocation, Watermarking

Monitoring ▶ Broadcast Operations Control Center

Published 10/20