NAGRAVISION
K U D E L S K I G R O U P

NAGRA CDN GATEKEEPER

Disrupt Piracy at the Edge — Without Impacting Your Customers

Pirates no longer need to break through firewalls — they're exploiting your own delivery infrastructure. With CDN Gatekeeper, NAGRAVISION delivers precision enforcement where it matters most: at the CDN edge. Whether it's credential sharing, content restreaming, or CDN leeching, our solution gives OTT streaming platforms the tools to identify, disrupt, and neutralize piracy threats without hurting legitimate viewers.

NAGRA CDN Gatekeeper equips OTT streaming platforms with edge-enforced disruption that targets pirate users without triggering alert or failover. Deployed within CDN environments like AWS, Akamai, Google, Broadpeak, the solution ingests real-time data from Forensic Watermarking and/or CDN Security Analytics and applies configurable disruptions (e.g., content blocking, alternate stream, bandwidth throttling, or segment corruption). Updates are pushed automatically via API, ensuring that infringement data transforms into action in minutes — not hours.

With support for both NexGuard Forensic Watermarking and CDN Security Analytics, CDN Gatekeeper is a critical layer of enforcement for the NAGRA Streaming Security suite, defending live sports and premium events across geographies and device types.

Solution Benefits

1. **Edge Enforcement without Collateral Damage:** Apply targeted restrictions only to pirate users, protecting stream quality for legitimate viewers.

2. **Multiple Disruption Modes:** Apply different types of disruption such as content blocking, bandwidth throttling, segment corruption, or alternate stream delivery in a way that avoids detection by pirate service operators—maximizing disruption while minimizing the risk of exposure.

3. **API-Driven Updates in Minutes:** Automatically push updated restriction lists to the CDN edge via secure APIs, ensuring real-time responsiveness during live events.

4. **Deploys Across Leading CDNs:** Works with AWS CloudFront, Akamai AMD, Google Service Extensions, and Broadpeak — with flexible deployment and updates at the CDN Edge.

5. **Integrated into Streaming Security Suite:** Correlate CDN Gatekeeper enforcement data with Multi-DRM, Application Security, and Watermarking for total streaming protection.

NAGRA CDN Gatekeeper

Turn threat intelligence into action — applying real-time restrictions at the CDN edge to disrupt pirate access without affecting legitimate users.

Real-Time Restriction List Generation
- Format entries supported for the restriction list will soon include WatermarkID, or SessionID, or AccountID, or DeviceID; Token signature; IP address; User agent or HTTP referrer
- List generated from NAGRA CDN Security Analytics and NexGuard Watermarking

CDN Edge Decisioning
- Enforces restrictions on all segments
- Web server, deployed in customer's own AWS account, to invoke APIs (Cloudfront, EdgeWorker, Service Extensions) and deploy updates at the CDN Edge
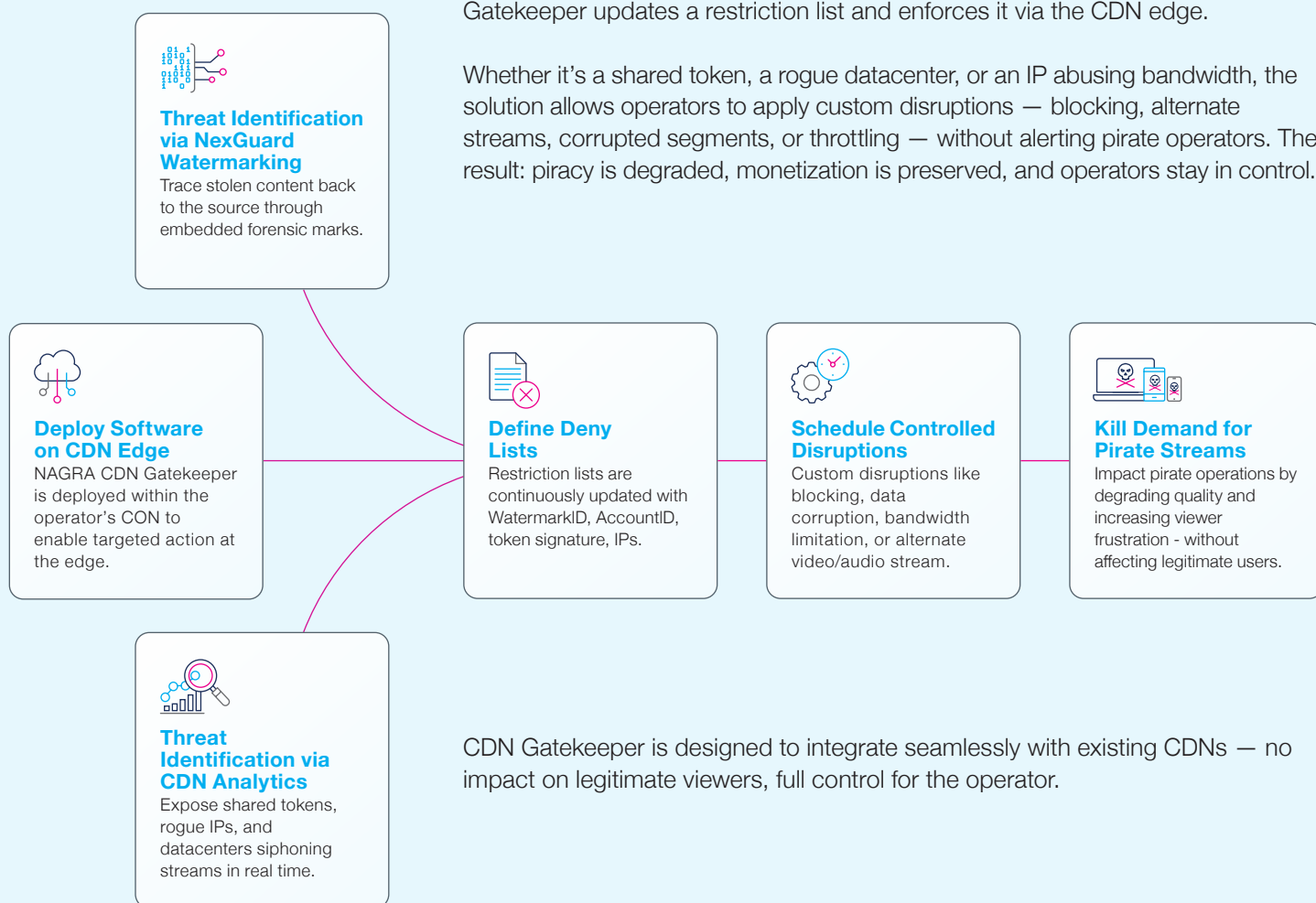
Disruption Origin Modules
- Executes disruptions like segment corruption or throttling
- Deployable via Docker images on AWS or on-prem

API & Automation Toolkit
- Enables WebUI and CLI-based updates
- Reduces deployment time and supports large-scale enforcement

How It Works

NAGRA CDN Gatekeeper deploys directly into your CDN environment to identify and disrupt pirate access — without affecting legitimate users. Once a threat is identified (via NexGuard Forensic Watermarking or CDN Security Analytics), CDN Gatekeeper updates a restriction list and enforces it via the CDN edge.

Whether it's a shared token, a rogue datacenter, or an IP abusing bandwidth, the solution allows operators to apply custom disruptions — blocking, alternate streams, corrupted segments, or throttling — without alerting pirate operators. The result: piracy is degraded, monetization is preserved, and operators stay in control.

Threat Identification via NexGuard Watermarking
Trace stolen content back to the source through embedded forensic marks.

Deploy Software on CDN Edge
NAGRA CDN Gatekeeper is deployed within the operator's CON to enable targeted action at the edge.

Threat Identification via CDN Analytics
Expose shared tokens, rogue IPs, and datacenters siphoning streams in real time.

Define Deny Lists
Restriction lists are continuously updated with WatermarkID, AccountID, token signature, IPs.

Schedule Controlled Disruptions
Custom disruptions like blocking, data corruption, bandwidth limitation, or alternate video/audio stream.

Kill Demand for Pirate Streams
Impact pirate operations by degrading quality and increasing viewer frustration - without affecting legitimate users.

CDN Gatekeeper is designed to integrate seamlessly with existing CDNs — no impact on legitimate viewers, full control for the operator.

Strategic Intelligence. Impactful Action.

The Kudelski Group brings decades of leadership in content protection, device security, and cybersecurity — with operations in 20+ countries, protecting over 500 service providers and 400 million devices worldwide. From studios tracing leaks to telcos defending live services and rights holders managing partner risk, NAGRA Streaming Security delivers targeted intelligence and decisive tools to match your mission.

If you'd like to learn more or explore next steps, please get in touch — we look forward to continuing the conversation.