DATADOG SOLUTION BRIEF

Safeguarding the streaming experience and audience trust

Top Media & Entertainment Companies Trust Datadog

PBS CANAL+ Vidio

The growing security challenge for digital media

Every frame of premium content represents both creative value and commercial risk. Piracy, credential theft, API abuse, and fraudulent playback access all undermine the customer's streaming experience and puts revenue at risk. From large-scale illegal streaming networks that cost rights holders billions each year to credential-stuffing campaigns and API abuse that flood authentication endpoints with malicious traffic, streaming platforms face threats that spread faster than what traditional defenses can contain. As distribution expands across devices, regions, and third-party content delivery networks (CDNs), the attack surface grows exponentially, and a single misconfigured entitlement API or leaked playback token can expose premium content to millions of unauthorized viewers within minutes.

Traditional monitoring tools such as WAFs, CDN logs, or Identity and Access Management (IAM) dashboards often operate in isolation, disconnected from one another and from the broader telemetry needed to understand how attacks compromise the streaming stack. This fragmentation delays timely detection of threats across APIs, applications, and infrastructure before they are contained. Spikes in login failures, scraping of playback endpoints, or geographic anomalies in entitlement validation are often recognized only after damage has occurred.

To safeguard intellectual property and preserve audience trust, streaming platforms need unified visibility across applications, APIs, infrastructure, and user behavior, with automated detection and response that move as quickly as content delivery itself.

Where protection breaks down

FRAGMENTED VISIBILITY ACROSS LAYERS

Authentication systems, playback applications, and CDNs each produce valuable telemetry, but rarely in context with one another, making it difficult to see how activity in one layer affects another. Without correlation across these layers, teams struggle to identify when a surge in API traffic represents legitimate growth or a coordinated credential-stuffing attack. This isolation keeps threat signals trapped within silos and delays response when seconds matter.

REACTIVE DETECTION AND MANUAL TRIAGE

The first generation of detection tools relied on static rules, fixed thresholds, and manual log reviews. This approach worked when infrastructures were largely monolithic and cloud resources changed infrequently. As streaming environments grew more distributed, with APIs scaling elastically and new services deploying continuously, static controls could no longer keep pace with real-time threats. They detect abuse only after tokens have been reused or playback has begun, forcing teams to respond post-compromise and driving up operational costs. Without automation and cross-system correlation, containment remains slow, fragmented, and incomplete.

COMPLEX AND EVOLVING COMPLIANCE REQUIREMENTS

Global streaming platforms operate under overlapping privacy and licensing frameworks such as GDPR, CCPA, SOC 2, and region-specific broadcast or data residency regulations. Tracking personally identifiable information (PII), entitlement tokens, and content rights data across thousands of APIs and microservices becomes nearly impossible without automation. A lack of unified auditability exposes organizations to compliance violations and potential fines.

Unifying observability and security for media

Every playback request, entitlement check, and API call contributes to the viewer experience and represents a potential attack surface. Datadog unifies observability, security, and compliance automation in a single platform, enabling media providers to protect both content delivery and viewer trust at a global scale.

Built on a secure architectural foundation that consolidates telemetry ingestion, access control, and automated workflows, Datadog connects security, reliability, and product teams through shared dashboards and coordinated response. This unified perspective allows teams to detect threats in real time, prioritize incidents intelligently, and respond automatically, all without impacting streaming performance or audience experience.

On this foundation, four integrated capabilities work together to safeguard content workflows, ensure compliance, and maintain trust across complex media ecosystems.

ENDPOINT AND WORKLOAD PROTECTION	
What it does	Protect workloads and infrastructure in real time
Powered by	Cloud Security Management (CSM)
How it works	– Collects kernel-level telemetry from hosts, containers, and processes to provide runtime and network context. – Correlates posture data with configuration insights to surface misconfigurations and vulnerabilities. – Detects malware, unauthorized binaries, and privilege escalation attempts in real time. – Enforces least-privilege access using RBAC and mTLS authentication, with automated alerts for violations.
Why it matters	Reduces attack surface and accelerates containment across distributed workloads.

THREAT AND ANOMALY DETECTION	
What it does	Detect and correlate threats across APIs and systems
Powered by	Cloud SIEM + Watchdog + Bits AI Security Analyst
How it works	– Ingests telemetry from APIs, CDNs, entitlement services, and playback applications to provide unified visibility across the streaming stack. – Watchdog uses machine learning to detect anomalies such as credential-stuffing, token replay, or sudden shifts in entitlement validation traffic. – Bits AI Security Analyst then autonomously triages Cloud SIEM signals, performing in-depth investigations grounded in the MITRE ATT&CK framework and Datadog threat research. – It identifies whether unusual activity stems from legitimate audience growth or coordinated credential or playback abuse, and provides clear, evidence-based remediation guidance for rapid response.
Why it matters	Detects threats faster, correlates events automatically, and shortens mean time to respond.

APPLICATION AND API PROTECTION	
What it does	Defend APIs and applications at runtime
Powered by	App and API Protection
How it works	– Captures application and API requests through embedded instrumentation within APM agents. – Evaluates payloads and parameters to identify OWASP Top 10 and logic-based risks. – Detects schema tampering, injection attacks, and abnormal behavior across distributed services. – Integrates with WAF and CDN controls to block or throttle malicious traffic instantly.
Why it matters	Maintains runtime security for critical APIs without adding latency or disrupting user experience.

SENSITIVE DATA SCANNING AND COMPLIANCE	
What it does	Identify and mask sensitive data across telemetry
Powered by	Sensitive Data Scanner
How it works	– Scans telemetry and logs to identify PII, tokens, and regulated data across environments. – Evaluates findings with ML-based classifiers to reduce false positives. – Enforces redaction, masking, and encryption (TLS 1.2+, AES-256) to maintain compliance and observability.
Why it matters	Ensures continuous compliance and protects user trust across global operations.

From reactive defense to proactive resilience

As streaming platforms grow more distributed and data rich, resilience depends on anticipating risk across every component of content delivery, not just detecting it after the fact. Proactive protection means automatically identifying and reducing exposure points before attackers can exploit them. This includes detecting entitlement drift, locking down over-permissive APIs, validating playback tokens against geographic or licensing rules, and ensuring sensitive telemetry never leaves approved regions. Datadog correlates infrastructure, API, and user telemetry in real time to highlight emerging anomalies and enforce preventive controls through automated workflows.

Datadog's unified approach transforms security from a reactive safeguard into an enabler of audience trust and business continuity. By aligning visibility, automation, and compliance across the delivery pipeline, organizations can prevent content leaks, enforce licensing compliance, and maintain protection without disrupting the viewer experience. With integrated observability and security, Datadog helps streaming providers reduce exposure, strengthen operational efficiency, and preserve trust at a global scale.

Take the next step

Safeguarding content and maintaining user trust require a unified view of security and observability. Datadog helps global media organizations detect threats early, enforce compliance automatically, and protect the viewer experience without sacrificing performance.

TRY DATADOG FREE