Buyer's Guide

Global CDN

Selecting a Modern, Security-First CDN That Protects and Accelerates Dynamic Web and API Traffic

Modern web applications, APIs, and microservices demand a CDN that delivers speed, resilience, and protection at scale. Traditional CDNs were built for static content and can't keep up with dynamic, Kubernetes-native workloads or Layer-7 threats.

This guide helps platform, DevOps, and security teams evaluate CDN solutions that accelerate content while embedding application-aware WAF, bot, and DDoS defenses without slowing users or operations.

Who This Guide Is For

This guide is ideal for teams that:

- ✓ Deliver content from multiple regions, clouds, or hybrid architectures
- ✓ Manage dynamic web applications, APIs, and microservices
- ✓ Face bot abuse, Layer-7 attacks, and unpredictable traffic spikes
- ✓ Require low-latency delivery with integrated security at the edge
- ✓ Want unified visibility without managing multiple consoles or appliances

1. Edge Performance & Global Acceleration

Content delivery must stay fast under any traffic spike.

- Does the CDN optimize static and dynamic content intelligently?
- Can it route REST, gRPC, and GraphQL requests to the fastest origin?
- Does it adapt automatically to congestion, latency, or regional failures?
- Can caching, load balancing, and traffic steering reduce origin load effectively?

2. Application & API-Aware Security

CDNs must stop attacks before they reach your origin.

- Does the CDN integrate inline WAF and bot protection at the edge?
- Can it detect API abuse, scraping, and credential stuffing patterns?
- Does it prevent zero-day exploits without impacting real users?
- Are threat intelligence and behavioral analytics used to tune protection automatically?

3. Bot & DDoS Defense

Modern bot traffic and Layer-7 attacks affect uptime and revenue.

- Can the CDN block automated attacks without CAPTCHA?
- Are rate limits adaptive and behavior-driven, not static thresholds?
- Does it detect low-and-slow and high-volume attack patterns?
- Can mitigation happen at the edge to prevent origin overload?

4. Deployment & Architectural Fit

Your CDN should integrate into your environment without disruption.

- Does it support Kubernetes-native, cloud, hybrid, and on-prem environments?
- Can it integrate with API gateways, service meshes, or edge proxies?
- Is deployment zero-code, zero-agent, and operationally frictionless?
- Does it maintain consistent policies across regions, clusters, and clouds?

5. Visibility, Analytics & Operational Insights

Understanding traffic, performance, and attacks is critical.

- ✓ Is there a unified dashboard for latency, cache, and security events?
- ✓ Can teams drill into edge, API, and region-level metrics in real time?
- ✓ Are logs exportable for audits, compliance, SIEM, and incident response?
- ✓ Does the CDN provide actionable insights for DevOps, SRE, and security teams?

Why Prophaze Global CDN

Prophaze Global CDN is built for modern web, API, and microservice platforms where performance and security must co-exist. By combining a globally distributed edge with AI-driven WAF, bot mitigation, and Layer-7 DDoS protection, it ensures traffic is served quickly while threats are absorbed before reaching your origin. Kubernetes-native, cloud-ready, and hybrid-capable, it eliminates tool sprawl, reduces operational overhead, and provides centralized, actionable insights for all teams.

- ✓ Intelligent, API-aware routing and caching at the edge
- ✓ Inline WAF, bot, and Layer-7 DDoS defense
- ✓ Multi-cloud, hybrid, and Kubernetes-native deployment
- ✓ Real-time analytics, anomaly detection, and global failover
- ✓ Zero-code deployment with minimal operational friction

About Prophaze

Prophaze provides an AI-driven WAAP platform that secures APIs and web applications against modern threats such as zero-day attacks, automated abuse, and Layer-7 floods. The platform delivers inline inspection, behavioral analysis, and adaptive enforcement across cloud, Kubernetes, hybrid, and on-prem environments without requiring SDKs or application code changes.

With centralized visibility, policy consistency, and 24/7 human-in-the-loop operations to reduce false positives, Prophaze helps teams protect API-driven environments while maintaining performance and operational efficiency.

CHOOSE HOW YOU WANT TO GET STARTED

Live Product Walkthrough
Custom Case Review
Architecture Consultation
30-min session

Schedule Demo

Start Free Trial