CONTINENT8 technologies

SECUREEDGE

connect8

CONNECT | SECUREEDGE

Built to deliver and defend iGaming.

The challenge

iGaming operators run some of the most demanding workloads on the web. Traffic surges around live sporting events, lobby pages that load tens of megabytes of casino assets per session, odds feeds scraped relentlessly by competitors and arbitrage bots, and login pages that attract more credential stuffing than almost any other sector. On top of that, operators have to enforce jurisdictional rules in real time and stay available through coordinated DDoS attacks aimed at extracting ransoms or disrupting major events.

Continent 8 SecureEdge is a managed **Content Delivery Network** and **Web Application Firewall** built for exactly this set of problems — running on Continent 8's private global network, purpose-built for the regulated betting and gaming industry.

#1
most targeted sector globally for four consecutive years

100+
Continent 8 network locations, including strong LatAm and Canadian coverage

10K+
A=active WAF rules covering OWASP, API abuse and bots

28+yrs
protecting iGaming operators, platforms and regulators

Why SecureEdge works for iGaming

Built for live event traffic
Edge caching absorbs the spikes that arrive with major football fixtures, F1 races and championship events, so origin systems stay responsive when betting volume peaks.

Account takeover defence
Behavioural fingerprinting, rate limiting and bot detection on login endpoints reduce credential stuffing — which targets gambling sites more than almost any other sector.

Jurisdictional enforcement at the edge
Geo-blocking, IP reputation filtering and Tor exit-node controls run at the edge, enforcing licence boundaries faster — and harder to bypass — than origin-level controls.

Casino and slot delivery at speed
Game graphics, audio and video cached close to the player reduce lobby drop-off and improve experience across regions where traditional CDNs underperform.

Odds and API protection
Deep inspection of REST, GraphQL and JSON traffic protects pricing feeds and trading APIs from scrapers, aggregators and arbitrage bots looking to drain commercial value.

Reach where it matters
Strong coverage in Brazil, Canada, the EU and APAC — including locations where mainstream CDNs are weak. New nodes added through Continen 8's global partnerships as markets open.

GET IN TOUCH
sales@continent8.com

Asia: +65 3165 4649
Europe: +44 1624 694625

Latin America: +54 11 5168 5637
North America: +1 514 461 5120

CONTINENT8 technologies

SECUREEDGE

connect8

CONNECT | SECUREEDGE

Use cases

01 · Live event traffic

Edge caching without origin strain.

Problem. Sports betting traffic spikes by an order of magnitude around major events, overwhelming origin and degrading in-play experience.

Cache hit rates routinely above 80% mean origin sees only a fraction of incoming requests, keeping in-play journeys responsive even when traffic surges several times above baseline.

02 · Casino and slots delivery

Game assets close to the player.

Problem. Modern slots and live-dealer games push tens of megabytes per session; drop-off rises sharply with every second of load time.

Image transformation, compression and format conversion at the edge cut payload size, and local PoPs cut round-trip times in markets where mainstream CDNs lack coverage.

03 · Live dealer streaming

Low-latency video, jurisdiction-aware.

Problem. Live-dealer studios need sub-second delivery to many regions at once, without leaking streams across licence boundaries.

Low-latency HLS and WebRTC distribution streams live studio feeds from the closest edge, with token authentication and geo-rules applied per session before bytes leave the node.

04 · Credential stuffing

Account takeover defence.

Problem. Gambling logins are among the most attacked endpoints on the web; stolen accounts are laundered or used to drain stored balances.

Behavioural fingerprinting, request-frequency analysis and known-scanner signatures block automated logins before they reach the application, with rate limiting absorbing volumetric stuffing.

05 · Odds and pricing APIs

Trading-feed protection.

Problem. Odds and price feeds are scraped at scale by competitors, aggregators and arbitrage operators, draining commercial advantage in seconds.

Deep inspection of REST, GraphQL and SOAP traffic detects malformed JSON, parameter pollution and abnormal access; per-endpoint limits protect high-value feeds without disrupting B2B partners.

06 · Licence boundaries

Geo-enforcement at the edge.

Problem. Operators serve different content, prices and promotions by jurisdiction, and face regulator scrutiny if players access services from outside licensed territories.

Geo-blocking, IP reputation filtering and Tor exit-node controls run at the edge before requests reach origin, with a single configuration enforcing licensing across every Continent 8 location.

GET IN TOUCH
sales@continent8.com

Asia: +65 3165 4649
Europe: +44 1624 694625

Latin America: +54 11 5168 5637
North America: +1 514 461 5120

CONTINENT8 technologies

SECUREEDGE

connect8

CONNECT | SECUREEDGE

Use cases

07 · Edge compute

Logic where the user is.

Problem. Personalisation, A/B testing, header rewrites and lightweight auth logic add round-trips to origin and slow the user journey.

Programmable edge workers run JavaScript at every PoP for header rewrites, A/B splits, session tagging and request authentication — without a trip back to origin.

08 · DevOps acceleration

Git caching and pipeline protection.

Problem. Global engineering teams pulling large Git repos and container images from a single region face slow builds and exposed CI endpoints.

Repository and artifact caching at the edge accelerates clones and pulls for distributed teams, while WAF and bot rules protect CI/CD endpoints, webhooks and registries from abuse.

09 · End-to-end on Continent 8

One provider, one path.

Problem. When edge, network and origin sit with three different providers, operators face finger-pointing during incidents and exposure to jurisdictions outside their control.

For operators whose origin is hosted with Continent 8, the entire path from player to application runs on Continent 8 infrastructure — independent of US-headquartered technology, removing exposure to the US CLOUD Act.

10 · PCI DSS 4.0

Compliance for payment flows.

Problem. Requirement 6.4.2, mandatory since March 2025, requires an automated technical solution in front of all public-facing web applications handling payments.

SecureEdge satisfies the PCI DSS 4.0 WAF requirement directly, with OWASP Top 10 coverage and reporting templates and SIEM integration aligned to the audit trail QSAs expect.

Built for iGaming

The only CDN and WAF designed around the traffic patterns, licence rules and threat profile of regulated betting and gaming.

Advanced edge, no VCL required

Industry-leading caching and acceleration, exposed through a simple portal and API. No specialist scripting language to learn before you can deploy.

One service, one provider

CDN, WAF and bot management delivered as one managed service, with a single contract, a single portal and a single support relationship.

GET IN TOUCH
sales@continent8.com

Asia: +65 3165 4649
Europe: +44 1624 694625

Latin America: +54 11 5168 5637
North America: +1 514 461 5120