CONTINENT8 technologies

SECUREEDGE

connect8

CONNECT | SECUREEDGE | FOR ENTERPRISE

Take back control of your web edge.

The challenge

Most large organisations now run their public web estate behind a CDN and a Web Application Firewall — but the market has consolidated around a handful of US-headquartered providers. That creates concentration risk, exposure to overseas legal frameworks like the US CLOUD Act, and a pricing dynamic where costs climb sharply once you depend on a single platform. PCI DSS 4.0, NIS2 and DORA increasingly require regulated sectors to demonstrate active management of web application risk and ICT supply-chain concentration.

Continent 8 SecureEdge is a managed **CDN** and **WAF** that runs entirely on Continent 8's private global network, with no reliance on US-headquartered technology providers. One service, one contract and one support team replace separate vendors for content delivery and web application security — with pricing that scales to your traffic rather than to vendor leverage.

100+
network locations across four continents on the Continent 8 private backbone

1M+
HTTP requests per second sustained per edge node

10K+
active WAF rules covering OWASP Top 10, APIs and bots

28+yrs
of managed infrastructure and cyber-defence experience

Why SecureEdge works for enterprise

Independent of US technology
No reliance on US-headquartered providers in the data path, removing exposure to the US CLOUD Act and easing compliance reviews under NIS2, DORA and similar frameworks.

Advanced edge, made simple
Industry-leading caching and acceleration capabilities exposed through a portal and API. No specialist edge scripting language to learn before you can deploy or change policy.

Continuous threat coverage
WAF rules written and applied as new threats emerge, with virtual patching shielding applications against known CVEs while teams schedule their own remediation.

Two vendors become one
CDN, WAF and bot management delivered as a single managed service, eliminating the integration and finger-pointing risks of running separate edge providers.

Predictable commercial model
Transparent pricing tied to traffic, with no surprise overage on adjacent features. Lower total cost than equivalent hyperscaler configurations at typical enterprise volumes.

Reach into underserved markets
Strong coverage in Brazil, Canada, parts of APAC and other markets where mainstream CDNs are thin. New locations added through Continent 8's global partnerships as business needs change.

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 | FOR ENTERPRISE

Use cases

01 · PCI DSS 4.0, NIS2 and DORA

Regulatory compliance, ready out of the box.

Problem. PCI DSS 4.0 Req 6.4.2 (mandatory March 2025) requires automated technical controls in front of public-facing web apps. NIS2 and DORA require managing ICT supply-chain concentration.

SecureEdge satisfies the PCI DSS 4.0 WAF requirement directly; for NIS2 and DORA it provides a defensible non-US alternative or second source. Templates align to PCI DSS 4.0, NIS2, DORA and ISO 27001, with SIEM integration via syslog, JSON, CEF.

02 · Vendor consolidation

Consolidating CDN and WAF.

Problem. Separate vendors for CDN and WAF increase cost, create configuration drift between layers, and leave ambiguity over who owns an incident.

Caching, acceleration, OWASP-class protection, API security and bot management run as one service on the same edge nodes. A single portal, API and support team replace the integration overhead of stitching two vendors together.

03 · Origin protection

Offload and virtual patching.

Problem. Origin infrastructure absorbs unnecessary load and attack surface when caching and inspection aren't done at the edge.

Cache hit rates routinely above 80% reduce origin demand. Virtual patching shields unpatched apps against known CVEs, and application-layer DDoS mitigation absorbs slow-POST, Slowloris and high-frequency floods before they reach origin.

04 · Incumbent migration

Switching CDN without the lock-in.

Problem. Edge providers price aggressively at acquisition and increase sharply once you depend on them, with switching costs deliberately engineered to be high.

DNS-based switchover, certificate import and gradual cutover by hostname or traffic percentage. API-driven configuration integrates with DevOps and CI/CD pipelines, so policies and cache rules live in code rather than a vendor portal.

05 · API security

REST, GraphQL and SOAP coverage.

Problem. APIs now carry more traffic than the web pages alongside them, but generic CDNs treat API traffic the same as static assets — missing abuse and injection patterns specific to API consumption.

Deep payload inspection of REST, GraphQL and SOAP traffic detects malformed JSON and parameter pollution. Caching, TLS termination and bot controls extend to API endpoints, with per-endpoint policy and rate limiting via portal or API.

06 · Underserved markets

Reach where mainstream CDNs are thin.

Problem. Mainstream CDNs have thin coverage in Brazil, Canada, parts of APAC and several emerging markets, degrading performance and weakening compliance positions for organisations operating there.

Continent 8 has strong direct presence in underserved markets, with the ability to deploy new edge locations through global partnerships when a market opens or a customer needs local data handling. Coverage is driven by your footprint, not a vendor's standard map.

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 | FOR ENTERPRISE

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

Traffic stays in one network.

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

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

10 · Media and large-asset delivery

Video, downloads, software updates.

Problem. Corporate video, software updates, training portals and large downloads strain origin and degrade experience without dedicated delivery infrastructure.

Low-latency HLS streaming, image transformation, compression and format conversion at the edge cut payload size before content reaches the user, with local PoPs reducing round-trip times in every region you serve.

Your data stays in our network

The platform runs entirely on Continent 8's private infrastructure. Traffic never transits third-party networks or US-headquartered providers.

Advanced edge, no VCL required

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

One service, one provider

CDN, WAF and bot management delivered as a single managed service, with a single contract, portal and 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

LINKEDIN TWITTER FACEBOOK YOUTUBE