HUMAN + GCP Load Balancer Callout

Protecting Cloud Applications at the Edge

Modern applications face relentless attacks from malicious bots—from credential stuffing and carding to scraping and fake account creation. Bots don't just drive up cloud costs—they degrade user experience, introduce security and fraud risks, and create costly operational overhead. Google Cloud Load Balancer customers can now filter out these threats at the edge.

The Challenge

Many organizations struggle to detect and block sophisticated bots at scale. Traditional tools like DDoS protection and Web Application Firewalls (WAFs) are essential, but they often fall short against sophisticated bot attacks.

The Joint Solution

Google Cloud Platform (GCP) Callout Enforcer, integrated with bot mitigation provided by the Human Defense Platform, offers real-time bot defense directly at the load balancer—before malicious traffic hits your backend.

Using GCP's Service Extensions, Layer 7 Load Balancers make a real-time callout to HUMAN Enforcer, which inspects incoming traffic and returns a decision to allow or block the request. This enables fast, centralized bot protection for all your GCP-hosted applications, without code changes or external proxies.

Benefits

Protect Your Infrastructure
Stops fraud, scraping, carding, and fake accounts at the edge.

Cut Cloud Costs
Reduces traffic to origin servers, saving on bandwidth, compute, and database operations.

Improve Customer Experience
Real users get seamless access while bots are silently filtered.

Simple Deployment
Protect all traffic at the load balancer layer—ideal for multi-app, multi-CDN environments.

Key Capabilities

GCP Native Deployment
Uses Load Balancer Service Extensions for clean, modern integration

No Code Changes Required
Deploys without modifying app infrastructure or pipelines

Real-Time Bot Detection
HUMAN inspects requests and returns allow/block decisions in milliseconds

Advanced Threat Intelligence
Leverages HUMAN's global telemetry to detect even stealthy or AI-driven bots

Centralized Traffic Filtering
Protects applications and APIs behind GCP Load Balancers

Ideal For

- **Retail & E-Commerce:** Improved checkout experience, lower fraud losses, fewer chargebacks, cost savings.
- **Financial Services & Fintech:** Pre-origin bot filtering, protection of sensitive banking APIs, real-time threat detection.
- **Government & Public Sector:** Reduced bot-driven fraud and alignment with NIST CSF
- **Healthcare & Telemedicine:** HIPAA-aligned protection, better patient experience, safeguarding telehealth platforms from abuse.
- **Education & EdTech:** Protects against fake account creation and abuse, ensures service availability during peak times.
- **Travel, Hospitality, and Ticketing:** Improved booking integrity, bot-blocking at the edge, protection of promotions.
- **Marketplaces & Platforms:** Protect platform trust and integrity, filter malicious traffic before it reaches microservices.

Solution Advantage

The joint solution of GCP Callout Enforcer and bot mitigation provided by HUMAN Security delivers powerful, real-time protection against automated threats directly at the load balancer layer. With HUMAN's advanced threat intelligence and GCP's scalable infrastructure, organizations gain a low-latency, high-performance defense that simplifies security operations and protects critical digital services.

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We verify that digital interactions, transactions, and connections are authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information please visit ***www.humansecurity.com***