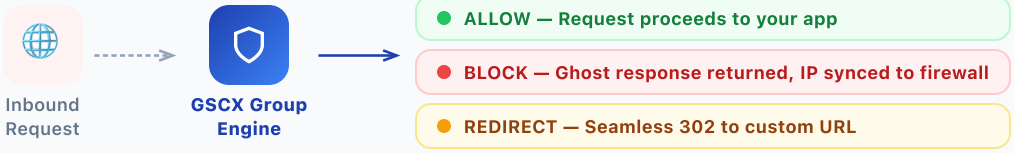
GSCX GROUP.SECURITY

MULTI-TENANT SECURITY DECISION ENGINE

Stop threats before they reach your application.

Enterprise-grade WAF protection, geofencing, real-time firewall sync,
and Ghost Response technology — all features on every plan.

WAF Protection · Ghost Response · Geo & IP Firewall · 🔥 Firewall Auto-Blocking



Rules evaluated in **priority order**. First match wins. No match → Default Policy applies. One API call from your backend.

CORE CAPABILITIES

Geo & IP Firewall
Country-level block/allow, CIDR ranges, geofence by radius. Works with Cloudflare, AWS, MaxMind.

Ghost Response System
Serve custom HTML, plain text, or 302 redirect — zero indication of the security decision to the attacker.

Firewall Auto-Blocking
BLOCK decisions instantly push UFW deny rules to all your linked servers. Network-layer protection, real time.

WAF-Style Rule Engine
Priority-ordered rules: IP lists, geo, geofence, rate limit, user-agent, path filter. Per-key default policies.

AI Bot Detection
UA fingerprinting, built-in bot signatures, regex patterns. Sliding-window rate limiting per IP or API key.

Analytics & Threat Logs
Real-time charts, top attacker IPs, threat scoring, full request logs with decision audit trail.

$4.88M
average cost of a data breach — IBM Security Report 2024

47%
of all internet traffic is bots — Imperva Bad Bot Report

194 days
average time to identify a breach without automated detection

< 1ms
GSCX Group Security decision latency — zero added overhead

⚠ THE RISK OF DOING NOTHING

- **No geo controls** — adversarial traffic from sanctioned regions hits your app unfiltered
- **Bots scrape freely** — credential stuffing, inventory hoarding, price scraping, and DDoS at machine speed
- **Attackers learn your stack** — every error response reveals your infrastructure, frameworks, and vulnerabilities
- **Breach costs compound** — regulatory fines, customer churn, incident response, and reputational damage add up fast
- **No audit trail** — when an incident occurs, you have no record of who accessed what, when, or from where

✓ PROTECTED BY GSCX GROUP SECURITY

- **Country + CIDR firewall** — deny entire regions or specific IP ranges before they touch a single line of your code
- **Ghost Response technology** — attackers receive a convincing decoy. They never know they're blocked — they simply never find you
- **Rate limiting + bot signatures** — sliding-window throttling and 100+ bot fingerprints stop automated attacks in real time
- **Network-layer sync** — BLOCK decisions instantly push UFW deny rules to every linked server. Threats stopped at the OS, not the app
- **Full audit trail** — every request, every decision, every rule match — logged, searchable, and exportable for compliance

WHY SECURITY TEAMS CHOOSE GSCX GROUP

UNIQUE TECHNOLOGY

The Only Platform with Ghost Response

No other API security platform offers Ghost Response. Instead of returning a 403 that tips off attackers, serve them believable decoy content — custom HTML, plain text, or a seamless redirect. Your real infrastructure stays invisible.

DEEPEST PROTECTION

App Layer + Network Layer — Simultaneously

Most security tools stop at the application layer. GSCX Group Security goes further — BLOCK decisions are instantly propagated as UFW firewall rules to every linked server. Threats are rejected at the OS network stack before they can retry.

INSTANT TIME-TO-VALUE

One API Call. Fully Protected in Minutes.

Integration is a single `POST /api/v1/check` from your backend. No agents to install, no SDK lock-in, no infrastructure changes. Works with any language or framework on day one.