# Lê Trọng Bằng – Hutech

# Proposal Workshop: Giải pháp Edge Security toàn diện với AWS WAF và CloudFront

## Executive Summary (Tóm tắt điều hành)

Trong bối cảnh hiện nay, các hệ thống web ngày càng đối mặt với các rủi ro bảo mật tại biên (edge) như: bot tấn công, DDoS, đánh cắp nội dung, truy cập trái phép, gây ảnh hưởng nghiêm trọng đến hiệu suất, độ tin cậy và trải nghiệm người dùng. Đặc biệt, các doanh nghiệp vận hành website công khai, API mở hoặc dịch vụ nội dung thường là mục tiêu chính của các loại hình tấn công này.

### **1.1 Vấn đề**

* Thiếu khả năng bảo vệ chủ động tại lớp biên (edge).
* Chi phí backend tăng cao do bot/scraper.
* Không kiểm soát được người dùng truy cập từ vùng địa lý không mong muốn.
* Thiếu giám sát và phản ứng tự động khi có sự cố.

### **1.2 Giải pháp đề xuất**

Chúng tôi đề xuất triển khai một giải pháp bảo mật edge toàn diện sử dụng AWS Native Services, cụ thể:

* AWS WAF: Xây dựng bộ quy tắc tùy chỉnh (custom rules) theo OWASP Top 10, geo-blocking, rate limiting, bot control.
* CloudFront: Làm lớp CDN bảo vệ và tối ưu truyền tải, kết hợp với HTTPS và header filtering.
* Lambda@Edge: Áp dụng xác thực JWT, CAPTCHA, logic tùy chỉnh chống bot tại biên.
* CloudWatch + Athena: Giám sát lưu lượng, phát hiện tấn công, tạo cảnh báo real-time.
* Signed URL / Token / IP filtering: Đảm bảo bảo vệ nội dung nhạy cảm.

### **1.3 Lợi ích kinh doanh và ROI:**

|  |  |  |
| --- | --- | --- |
| **Yếu tố** | **Trước khi áp dụng** | **Sau khi áp dụng** |
| Tỷ lệ bot traffic | 30–50% | Giảm còn <5% |
| Latency truy cập | Không ổn định, ~200ms+ | Ổn định <50ms nhờ CDN và cache |
| Chi phí backend EC2/API | Cao, scale liên tục | Giảm ~30–50% do giảm tải |
| Rủi ro bảo mật | Cao, không được giám sát thường xuyên | Giảm thiểu, có cảnh báo và phân tích tự động |

**ROI dự kiến**: hoàn vốn sau 3–4 tháng, tiết kiệm vận hành dài hạn, tăng uptime → giữ chân khách hàng tốt hơn.

### **1.4 Nguồn đầu tư và lộ trình thời gian**

* Chi phí ban đầu (one-time): ~600 USD cho thiết kế, triển khai và test.
* Chi phí duy trì hàng tháng: ~80–100 USD (CloudFront, WAF, Lambda, log, monitoring).
* Thời gian triển khai: 4 tuần với 4 pha chính (WAF, CloudFront, Lambda@Edge, Monitoring).

### **1.5 Chỉ số thành công kỳ vọng**

|  |  |
| --- | --- |
| **Chỉ số** | **Giá trị kỳ vọng** |
| Latency CDN | < 50ms toàn cầu |
| Tỷ lệ bot bị chặn | > 95% |
| Uptime | ≥ 99.99% |
| Cache hit ratio | ≥ 80% |
| Thời gian phản ứng sự cố | < 5 phút |

## 2. Problem Statement (Tuyên bố vấn đề)

**Mục tiêu**: Định nghĩa rõ ràng vấn đề cần giải quyết trong việc triển khai giải pháp bảo mật biên (Edge Security) sử dụng AWS.

### **2.1 Current Situation Analysis**

Hiện nay, nhiều ứng dụng web đang được triển khai trực tiếp trên nền tảng đám mây hoặc sử dụng CDN như CloudFront để phân phối nội dung toàn cầu. Tuy nhiên, các tổ chức thường thiếu các cơ chế bảo mật hiệu quả ở tầng edge (biên mạng), nơi tiếp xúc trực tiếp với lưu lượng từ người dùng trên internet.

Trong khi các dịch vụ như AWS WAF và CloudFront cung cấp nền tảng mạnh mẽ cho bảo mật biên, thực tế triển khai vẫn còn hạn chế vì:

Chưa tận dụng đầy đủ các khả năng như bot mitigation, rate-based rules, lambda@edge custom logic.

Không có chiến lược thống nhất trong việc kết hợp security + performance + cost.

Phản ứng sự cố chưa hiệu quả vì thiếu cơ chế giám sát và phản hồi theo thời gian thực.

### **2.2 Pain Points Identification (with Quantified Impact)**

|  |  |
| --- | --- |
| **Vấn đề** | **Tác động cụ thể** |
| Lưu lượng tấn công DDoS và bot ngày càng gia tăng | Gây quá tải hạ tầng, tăng chi phí vận hành lên đến 30–50% trong các đợt cao điểm |
| Nội dung dễ bị scraping hoặc copy trái phép | Gây rò rỉ tài sản số, ảnh hưởng tới doanh thu và thương hiệu |
| Quy tắc bảo mật thiếu tùy biến, không thích ứng với các mối đe dọa mới | Không ngăn chặn kịp thời các kiểu tấn công zero-day hoặc evasive bot |
| Không có alerting hoặc dashboard theo thời gian thực | Mất 4–12 giờ để phát hiện và xử lý sự cố |

### **2.3 Stakeholders Affected và Their Concerns**

|  |  |
| --- | --- |
| **Stakeholder** | **Mối quan tâm chính** |
| Đội bảo mật (Security Team) | Cần có hệ thống ngăn chặn bot/tấn công chính xác, dễ cập nhật, và phản hồi nhanh |
| DevOps / SRE | Cần đảm bảo hệ thống ổn định, không ảnh hưởng hiệu năng hoặc tăng chi phí |
| Ban điều hành /Chủ sản phẩm | Quan tâm đến rủi ro bảo mật gây ảnh hưởng đến doanh thu, uy tín, và chi phí phát sinh |
| Người dùng cuối | Mong muốn hệ thống phản hồi nhanh, không bị chậm do filter hoặc challenge không cần thiết |

### **2.4 Business Consequences của Inaction**

Tăng rủi ro bảo mật: Không triển khai edge security có thể dẫn đến data leak, DDoS downtime, hoặc phá hoại thương hiệu.

Tăng chi phí AWS và vận hành: Bot traffic có thể chiếm hơn 40% lưu lượng CloudFront, gây tăng chi phí CDN và origin.

Giảm hiệu suất trải nghiệm người dùng: Tăng thời gian phản hồi nếu không tối ưu edge logic, ảnh hưởng đến SEO và tỷ lệ giữ chân người dùng.

Khó đáp ứng tiêu chuẩn tuân thủ (compliance) như GDPR, SOC 2 nếu không có cơ chế bảo vệ dữ liệu sớm từ tầng edge.

### **2.5 Market Opportunity Tăng trưởng thị trường bảo mật đám mây:**

Theo Gartner, chi tiêu cho bảo mật cloud dự kiến đạt $18.5 tỷ USD vào năm 2025. AWS WAF và CloudFront ngày càng phổ biến trong các doanh nghiệp vừa và lớn — mở ra cơ hội tư vấn và triển khai giải pháp tối ưu.

Bot detection và edge computing đang trở thành xu hướng chính — doanh nghiệp đầu tư sớm sẽ có lợi thế cạnh tranh rõ ràng trong việc bảo vệ tài sản số và tối ưu chi phí vận hành.

## 3. Solution Architecture (Kiến trúc giải pháp)

### **3.1 Kiến trúc tổng thể:**

[User] → [CloudFront]

↓

[AWS WAF - ACL Ruleset]

↓

[Lambda@Edge - Bot Detection / Auth]

↓

[S3 Web]

### **3.2 Dịch vụ AWS sử dụng**:

|  |  |
| --- | --- |
| **Dịch vụ AWS** | **Vai trò/ Lý do sử dụng** |
| S3 (Static Website) | Lưu trữ nội dung tĩnh |
| Amazon CloudFront | DN phân phối nội dung nhanh, bảo vệ TLS, kết nối với WAF và Lambda@Edge |
| AWS WAF | Thiết lập ACL để chặn bot, chặn IP, geo-blocking, bảo vệ OWASP Top 10 |
| Lambda@Edge | Logic tùy chỉnh: phân tích User-Agent, xác thực JWT, redirect CAPTCHA nếu nghi ngờ bot |
| CloudWatch Logs | Ghi nhận mọi truy cập, request bị chặn, sử dụng cho alert |
| Athena | Truy vấn log WAF và CloudFront để phát hiện mẫu truy cập xấu |
| AWS Shield (Basic) | Tự động bảo vệ khỏi DDoS cơ bản |

### **3.3 Tương tác giữa các thành phần và luồng dữ liệu**

- Người dùng gửi request đến website thông qua CloudFront.

- CloudFront thực hiện TLS termination và chuyển tiếp request đến AWS WAF.

- WAF kiểm tra:

IP (IPSet hoặc block list)

Header, User-Agent, query pattern

GeoMatch

Tốc độ truy cập (Rate-based rules)

Bot signatures (nếu bật Bot Control)

* Nếu vượt qua WAF, request được chuyển tới Lambda@Edge (viewer request hoặc origin request):

Kiểm tra bot logic nâng cao (bằng Regex, token…)

Kiểm tra JWT hoặc signed URL

Thêm header theo dõi hoặc xác thực

* Nếu hợp lệ, request đi tiếp đến Origin (S3, ALB hoặc API Gateway).
* Phản hồi được trả ngược lại qua CloudFront về người dùng.
* Toàn bộ log request và action được lưu vào CloudWatch Logs / S3.
* Athena được dùng để truy vấn log theo mẫu hoặc cảnh báo bất thường

### **3.4 Kiến trúc bảo mật và tuân thủ**

* Xác thực tại Edge: Dùng JWT/signed URL để xác minh request.
* Bot detection: Kết hợp rule-based detection tại WAF và pattern-based với Lambda@Edge.
* Rate Limiting: Giới hạn số lượng request theo IP/time để chống flood.
* Geo-blocking: Chặn truy cập từ quốc gia không được phép.
* Header control: Xóa hoặc inject header độc hại (XSS, header injection).
* Tuân thủ bảo mật: Áp dụng theo OWASP Top 10, GDPR (qua chặn theo vùng), ISO 27001 (log retention, kiểm tra truy cập).

### **3.5 Khả năng mở rộng và hiệu suất**

* Auto scale toàn cầu: CloudFront tự động phân phối và cache nội dung ở 400+ edge location trên toàn cầu.
* Lambda@Edge chạy tại điểm gần người dùng, không cần provision thêm compute.
* Caching tại edge: Giảm tải backend đáng kể (trung bình ~80% request không cần gọi đến origin).
* Chi phí tối ưu: Không cần EC2/nginx để xử lý bảo mật, mọi logic xử lý tại edge native.

## 4. Technical Implementation (Triển khai kỹ thuật)

### **4.1 Giai đoạn triển khai và kết quả bàn giao**

|  |  |  |
| --- | --- | --- |
| Giai đoạn | Hoạt động chính | Kết quả bàn giao |
| 1 | Thiết lập và thử nghiệm AWS WAF (WebACL) | RuleSet chặn OWASP, geo, bot, rate limit hoạt động đúng |
| 2 | Cấu hình CloudFront tích hợp với origin (S3) | CDN hoạt động, truy cập TLS, định tuyến hợp lệ |
| 3 | Viết và triển khai Lambda@Edge xử lý bảo mật tùy chỉnh | CAPTCHA, JWT check, bot logic hoạt động đúng tại edge |
| 4 | Thiết lập logging, phân tích log và cảnh báo | CloudWatch/Athena phân tích request xấu, SNS cảnh báo |

### **4.2 Yêu cầu kĩ thuật**

|  |  |
| --- | --- |
| **Hạng mục** | **Chi tiết** |
| Compute | Lambda@Edge chạy tại viewer/origin request (128–512MB RAM) |
| Storage | S3 lưu nội dung tĩnh, S3 log bucket lưu access log |
| Network | CloudFront phân phối toàn cầu, HTTPS bắt buộc, Origin Access Control |
| Security | IAM roles cho Lambda, WAF logging permission, bucket policy hạn chế truy cập |
| Logging | WAF logging → CloudWatch Logs → S3 → Athena |

### **4.3 Phương pháp phát triển và quy trình**

* Mô hình phát triển: Triển khai theo mô hình IaC (Infrastructure as Code) dùng AWS CloudFormation/CDK hoặc Terraform.
* Quản lý phiên bản: Git (kết hợp GitHub/GitLab), CI/CD với CodePipeline hoặc GitHub Actions.
* Môi trường tách biệt: Dev → Staging → Production để kiểm thử WAF rules, Lambda functions trước khi áp dụng thật.

### **4.4 Chiến lược kiểm thử**

|  |  |
| --- | --- |
| **Loại kiểm thử** | **Nội dung kiểm thử cụ thể** |
| **Unit Test** | Kiểm tra logic trong Lambda@Edge: JWT validate, bot detection |
| **Integration Test** | Kiểm tra tương tác giữa CloudFront ↔ WAF ↔ Lambda ↔ Origin |
| **Performance Test** | Dùng JMeter/K6 gửi 1K–10K requests/s để đánh giá latency, blocking |
| **PenTest/Security** | Kiểm tra tấn công XSS, SQLi, Bot fuzzing với tool như OWASP ZAP |
| **Failover Test** | Tắt Lambda để đảm bảo hệ thống fallback hợp lý |

### **4.5 Kế hoạch triển khai và rollback**

* **Triển khai:**

Mỗi WAF rule được thử nghiệm độc lập trong Staging ACL

Lambda@Edge được deploy lên region us-east-1 với các phiên bản canary

Thay đổi được đẩy thông qua pipeline CI/CD có xác nhận

* **Rollback:**

Sử dụng versioned CloudFormation stack

Lambda@Edge giữ lại bản release gần nhất (alias-based rollback)

CloudFront hỗ trợ rollback config thông qua distribution version history

### **4.6 Quản lý cấu hình (Configuration Management)**

|  |  |
| --- | --- |
| **Hệ thống cấu hình** | **Phương pháp quản lý** |
| WAF ACL | CloudFormation YAML hoặc AWS Managed Rules + Custom |
| Lambda@Edge | Code lưu trữ Git + tự động build qua CI/CD |
| Origin Setup | Quản lý cấu hình S3 bucket policy, API Gateway resource |
| Logging / Alerts | Terraform / CLI script tạo log group, Athena table |

## 5. Timeline & Milestones (Lộ trình và các mốc)

### **5.1 Tổng quan lộ trình triển khai: 4 tuần**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tuần** | **Giai đoạn** | **Hoạt động chính** | **Kết quả đầu ra (Milestone)** |
| 1 | Phân tích & Thiết kế | - Xác định yêu cầu- Thiết kế kiến trúc- Kịch bản tấn công edge phổ biến | Tài liệu thiết kế, sơ đồ kiến trúc, danh sách rule ban đầu |
| 2 | Cấu hình WAF & CloudFront | - Tạo CloudFront Distribution- Thiết lập AWS WAF ruleset + Geo-blocking | CloudFront hoạt động, WAF ngăn chặn bot & IP xấu |
| 3 | Triển khai Lambda@Edge | - Viết và deploy chức năng (JWT check, captcha)- Test trên Staging | Lambda hoạt động đúng, redirect & phân tích request hợp lệ |
| 4 | Logging & Giám sát | - Bật logging (CloudWatch, Athena)- Viết truy vấn và cảnh báo bot/suspicious | Dashboard và cảnh báo hoạt động |

### **5.2 Critical Path (Đường găng)**

* Triển khai WAF ruleset là điều kiện tiên quyết để test Lambda@Edge
* CloudFront distribution phải được tạo và phân phối DNS trước khi có thể thử nghiệm ở bước 3
* Logging chỉ có ý nghĩa khi request thực tế được đưa qua edge → phụ thuộc các bước trước

Đường găng:

WAF + CloudFront cấu hình đúng → Lambda@Edge triển khai chính xác → Logging → Monitoring

### **5.3 Phụ thuộc và thứ tự hợp lý:**

|  |  |
| --- | --- |
| **Tác vụ cần hoàn thành trước** | **Phụ thuộc của nó (bước tiếp theo)** |
| CloudFront được cấu hình | Lambda@Edge deploy vào Viewer Request |
| WAF hoạt động với IP set | Test load traffic với script |
| Lambda@Edge viết xong | Triển khai chức năng xác thực + redirect |
| Bật logging + logs đẩy về S3 | Truy vấn bằng Athena |

### **5.4 Thời gian dự phòng và quản lý rủi ro**

* Dự phòng 2–3 ngày để:

Xử lý lỗi cấu hình CloudFront (Propagation chậm)

Điều chỉnh rule WAF nếu block sai

Khắc phục lỗi Lambda (nếu cần rollback)

* Áp dụng mô hình staging / production tách biệt để tránh ảnh hưởng người dùng thật trong quá trình thử nghiệm

## 6. Budget Estimation (Ngân sách)

### **6.1 Chi phí hạ tầng AWS (ước tính hàng tháng)**

|  |  |  |
| --- | --- | --- |
| **Dịch vụ AWS** | **Mô tả sử dụng** | **Ước tính chi phí/tháng** |
| CloudFront | 1TB data transfer, ~1 triệu requests | ~$45–60 |
| AWS WAF | 1 WebACL, 10 custom rules, 1 managed rule set | ~$25–30 |
| Lambda@Edge | ~1 triệu invocations/tháng, thời gian chạy ~100ms | ~$5–10 |
| CloudWatch Logs | 10 GB log lưu trữ, 10 triệu events | ~$5 |
| Athena + S3 log bucket | Truy vấn 20GB/tháng, lưu logs 1 tháng | ~$5–10 |

|  |  |
| --- | --- |
| Tổng cộng (theo tháng) | ~$85 - 115 |
| Tổng chi phí hạ tầng trong 1 năm(ước tính) | ~$1,100 – 1,400 |

### **6.2 Chi phí vận hành (hàng tháng)**

Theo dõi logs, bảo trì rule WAF, cập nhật blacklist IPs: ~4–6 giờ/tháng

Ước tính công vận hành: ~$100–150/tháng nếu thuê ngoài hoặc tính nội bộ

### **6.3 Chiến lược tối ưu chi phí**

|  |  |
| --- | --- |
| **Hướng tối ưu** | **Mô tả cụ thể** |
| Dùng rule managed miễn phí | Dùng AWS managed rules (e.g. AWS-AWSManagedRulesCommonRuleSet) |
| Cache tốt tại CloudFront | Tối ưu TTL, use signed URL cho nội dung private |
| Filter log hợp lý | Giới hạn log cần thiết, đặt retention hợp lý |
| Chia traffic theo mức ưu tiên | Phân biệt traffic quốc tế, traffic nội vùng để điều phối hợp lý |
| IaC + CI/CD tự động | Giảm công sức vận hành bằng quy trình hóa và tự động hóa triển khai |

## 7. Risk Assessment (Đánh giá rủi ro)

### **7.1 Xác định rủi ro**

|  |  |
| --- | --- |
| **Loại rủi ro** | **Mô tả cụ thể** |
| Kỹ thuật | WAF block nhầm request hợp lệ; Lambda@Edge lỗi logic; propagation chậm CloudFront |
| Vận hành | Logging không đầy đủ; chi phí logs tăng nhanh; thiếu cảnh báo kịp thời |
| Kinh doanh | Người dùng bị chặn ngoài ý muốn → ảnh hưởng trải nghiệm, mất khách hàng |
| Bảo mật | JWT xác thực lỗi → rò rỉ nội dung; thiếu bot protection → bị khai thác lại |
| Con người | Dev cấu hình sai WAF/Lambda, rollback muộn hoặc sai môi trường |

* 1. **Đánh giá tác động và xác suất (Risk Matrix)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Rủi ro** | **Mức độ tác động** | **Xác suất xảy ra** | **Mức độ ưu tiên** |
| Block nhầm request hợp lệ | Cao | Trung | Cao |
| Lambda@Edge lỗi logic | Trung | Thấp | Trung |
| Logging quá nhiều gây tăng chi phí | Trung | Trung | Trung |
| Xác thực JWT sai | Cao | Thấp | Trung |
| Thiếu cảnh báo khi có bot traffic tăng | Trung | Trung | Trung |

* 1. **Chiến lược giảm thiểu rủi ro**

|  |  |
| --- | --- |
| **Rủi ro** | **Biện pháp giảm thiểu cụ thể** |
| Block nhầm request | Triển khai rule trong môi trường Staging trước Production; log-only mode |
| Lambda@Edge sai logic | Viết Unit test kỹ, kiểm thử staging; sử dụng phiên bản rollback được |
| Logs quá nhiều | Thiết lập filter log hợp lý, giới hạn retention, nén log về S3 |
| JWT xác thực sai | Kiểm thử với nhiều luồng xác thực; fallback to anonymous view (tùy chính sách) |
| Thiếu cảnh báo | Kết hợp CloudWatch Alerts + SNS, test giả lập bot request thường xuyên |

* 1. **Kế hoạch ứng phó (Contingency Plans)**

|  |  |
| --- | --- |
| **Tình huống** | **Hành động ứng phó ngay lập tức** |
| Rule chặn sai user thật | Revert WAF ruleset về bản stable (sử dụng versioning) |
| Lambda không xử lý được request | Disable Lambda@Edge temporarily, dùng fallback header |
| Logs tăng bất thường | Giảm mức độ log, chuyển sang sampling, tăng phân tích Athena |
| Bot vượt qua xác thực | Bật CAPTCHA, chặn IP tạm thời qua WAF IPSet |

* 1. **Quy trình giám sát và cảnh báo**

|  |  |  |
| --- | --- | --- |
| **Thành phần giám sát** | **Công cụ sử dụng** | **Cảnh báo qua** |
| WAF request logs | AWS CloudWatch Logs + Athena | SNS / Email / Slack |
| Lambda error rate | CloudWatch Metrics + Alarm | SNS / Email |
| Bot traffic spike | Custom metric + threshold | Alert system |
| Chi phí tăng bất thường | AWS Budgets + Cost Anomaly Detection | Email / Billing alerts |

## 8. Expected Outcomes (Kết quả mong đợi)

### **8.1. Chỉ số thành công (Success Metrics)**

|  |  |
| --- | --- |
| **Hạng mục** | **Mục tiêu cụ thể** |
| Latency CloudFront | < 50ms (toàn cầu) |
| Tỷ lệ truy cập bot giảm | > 95% request bot bị chặn hoặc redirect |
| Uptime hệ thống | ≥ 99.99% |
| Tỷ lệ cache hit | > 80% (giảm tải backend gốc) |
| Thời gian phản ứng sự cố | < 5 phút thông qua cảnh báo và tự động hóa giám sát |

### **8.2. Lợi ích ngắn hạn (0–6 tháng)**

* Nhanh chóng chặn traffic xấu từ bot, scraper, IP lạ hoặc theo vùng địa lý.
* Giảm tải cho backend, giúp giảm chi phí compute/API và tối ưu hiệu suất.
* Tăng độ ổn định, giúp hệ thống không bị sập khi có spike traffic bất thường.
* Người dùng thật truy cập nhanh hơn nhờ cache và phân phối qua CloudFront.

### **8.3. Lợi ích trung hạn (6–18 tháng)**

* Hệ thống tự động bảo vệ và phản ứng trước các hành vi tấn công phổ biến (OWASP).
* Cải thiện trải nghiệm người dùng với giao diện phản hồi nhanh, độ trễ thấp.
* Giảm chi phí vận hành hằng tháng nhờ tối ưu tài nguyên sử dụng.
* Dễ dàng mở rộng khi traffic tăng hoặc cần hỗ trợ nhiều vùng địa lý hơn.

### **8.4. Giá trị dài hạn (18+ tháng)**

* Doanh nghiệp sở hữu một nền tảng edge security hiện đại, có thể tái sử dụng cho các dự án mới.
* Giảm thiểu rủi ro bảo mật dài hạn, bảo vệ thương hiệu và dữ liệu người dùng.
* Nâng cao năng lực vận hành DevSecOps, ứng dụng tốt AWS-native cho bảo mật biên.
* Khả năng tích hợp SIEM/SOAR hoặc các hệ thống bảo mật doanh nghiệp sau này.
  1. **Cải thiện trải nghiệm người dùng**

|  |  |
| --- | --- |
| **Trước triển khai** | **Sau triển khai** |
| Latency không ổn định | Truy cập nhanh, ổn định ở mọi khu vực qua CloudFront |
| Dễ bị chặn do overload backend | Hệ thống hoạt động mượt, có cache và bảo vệ chủ động |
| Khó kiểm soát hành vi bot | Giao diện an toàn, CAPTCHA linh hoạt và xác thực thông minh |

### **8.6. Năng lực chiến lược đạt được**

* Thiết lập mô hình Edge Security chuẩn AWS, có thể chuẩn hóa cho nhiều môi trường.
* Nâng cấp nhận thức và kỹ năng bảo mật cho đội ngũ kỹ thuật.
* Tăng khả năng đáp ứng các tiêu chuẩn compliance và audit (VD: ISO 27001, GDPR).
* Là tiền đề để tích hợp các hệ thống bảo mật nâng cao như WAFv2, GuardDuty, Firewall Manager.