GIỚI THIỆU
BỘ DỊCH VỤ TƯỜNG LỬA CHO ỨNG DỤNG WEB

(Hoạt động tăng tốc, phòng chống tấn công và bảo vệ dịch vụ)

14 May, 2025

CDN và Dịch vụ bảo mật điện toán đám mây Cloud Security

Mạng Lưới Hạ Tầng Toàn Cầu

200,000+
Máy chủ trên toàn cầu

2,800+
PoPs

200Tbps+
Băng thông CDN toàn cầu

70+
Quốc gia và các vùng lãnh thổ

200+
Đối tác ISP toàn cầu

15Tbps+
Thông lượng chống tấn công của các trung tâm Scrubbing

20+
Trung tâm Scrubbing

1,000PB+
Dung lượng lưu trữ

Mạng Lưới Hạ Tầng Ở Việt Nam

viettel
Theo cách của bạn

VNPT

FPT Telecom

HITC
Power your breakthroughs

SCTV

10
PoPs

2
Trung tâm Scrubbing

1Tbps+
Băng thông tổng

Kinh nghiệm bảo mật

3,336,701,369

Số lượng tấn công trung bình được ngăn chặn mỗi ngày.

90%

Hơn 90% các domain kích hoạt tính năng bảo vệ WAF chạy ở chế độ chặn

34.7M RPS

Ghi nhận số lượng request tấn công DDoS L7 đã được xử lý thành công

2.09Tbps

Ghi nhận băng thông tấn công DDoS L3/4 lớn nhất đã được xử lý thành công.

1 Billion+

Thư viện các mẫu tấn công được cập nhật tự động

100+ Security Experts

Đảm bảo hoạt động và chất lượng dịch vụ chạy ổn định

Các Khách Hàng Tiêu Biểu Theo Lĩnh Vực

Tài chính & Ngân hàng	JCB, McLarens, UOB, FXCM, AXA, NSI National Securities
Giáo dục trực tuyến	University of Cambridge, Học viện Ngân hàng, Đại học Kinh tế Quốc dân, Zhejiang University, seewo 希沃, NCET
Sản xuất	Petrolimex, KIOXIA, SAMSUNG, TOYOTA, Busch Vacuum Solutions, Haier
Truyền thông & Giải trí	Cốc Cốc, TikTok, VOV Giao Thông FM.91MHz, K+, today, Asiasoft, CCTV, itel, TEN NIS
Trò chơi trực tuyến	VTC Online, GAMEON, Nintendo, OUTFIT7, KT Koei Tecmo America Corp.
Thương mại điện tử	PANDORA, Groupe Casino, RIVER ISLAND, ebay, alexanderwang
Công nghệ & Phần mềm	TOSHIBA, GMO Internet Group, KDDI, 360, ByteDance
Y tế & Du lịch	HOSTELWORLD, TOKYU HOTELS, JR East, FREIGHTOS, Knight Frank, Ctrip

Bảo Mật Đám Mây

Sự phát triển của Giải pháp bảo mật

Phương pháp bảo vệ truyền thống

Lợi điểm

- Đặc biệt phù hợp với những khách hàng "Bảo thủ" không chịu chuyển đổi lên cloud.

Bất cập

- Vận hành và bảo trì phức tạp
- Chi phí đầu tư lớn
- Không thể mở rộng ngay lập tức theo nhu cầu

Cloud Security (sản phẩm đơn lẻ)

Lợi điểm

- Mở rộng nhanh theo nhu cầu, dễ dàng triển khai

Bất cập

- Các sản phẩm bảo mật độc lập và tách biệt
- Không đồng nhất bảng biểu, nhật ký
- Phức tạp trong vận hành bảo mật

WAAP một bộ giải pháp dịch vụ tường lửa cho ứng dụng Web

Một vòng tròn quản lý rủi ro cho các ứng dụng web và API

- Nền tảng đồng nhất
- Quản trị dễ dàng
- Bảo vệ và quản lý bằng công nghệ AI
- Mở rộng nhanh theo nhu cầu, dễ dàng triển khai

Các lớp Giải pháp Bảo mật

Client

Truy cập hợp lệ

Truy cập tấn công

Cloud Security

1st Line of Defense

- DDoS Mitigation
- Cloud WAF
- Bot Management
- API Security
- Security Service

1st
Bảo mật đám mây

Hệ thống máy chủ

Threat Intelligence Sharing

2nd Line of Defense

- Firewall
- WAF hardware

2nd
Bảo mật phần cứng

3rd Line of Defense

- Phát hiện toàn bộ các lưu lượng truy cập giả mạo bằng thuật toán phân tích chuyên sâu.
- Ví dụ: IDS, VDS

3rd
Phát hiện giả mạo

4th Line of Defense

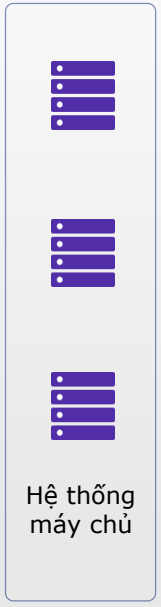
- Bảo vệ Host
- Bảo vệ Container

4th
Bảo vệ Host

5th Line of Defense

- Đánh giá hoạt động của ứng dụng bằng phương pháp tự động hoặc thủ công.
- Ví dụ: xử lý lỗi, dịch vụ VS, PT

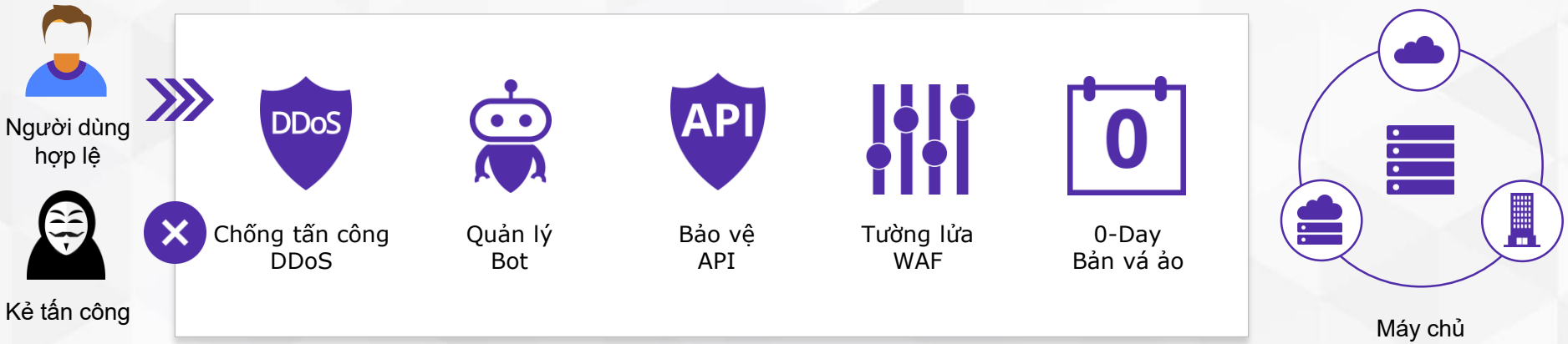
5th
Bảo vệ ứng dụng



Hệ thống máy chủ

Threat IP list for blocking on cloud

Các lớp tính năng Bảo mật



Bảo vệ kết hợp

Kết hợp các tính năng bảo vệ trong cùng một bộ giải pháp bảo mật, giúp nâng cao khả năng bảo vệ và phòng chống tấn công

Mở rộng nhanh chóng

Mở rộng nhanh chóng để ứng phó với các cuộc tấn công bất ngờ với quy mô lớn

L3-L7

Bảo vệ rộng rãi

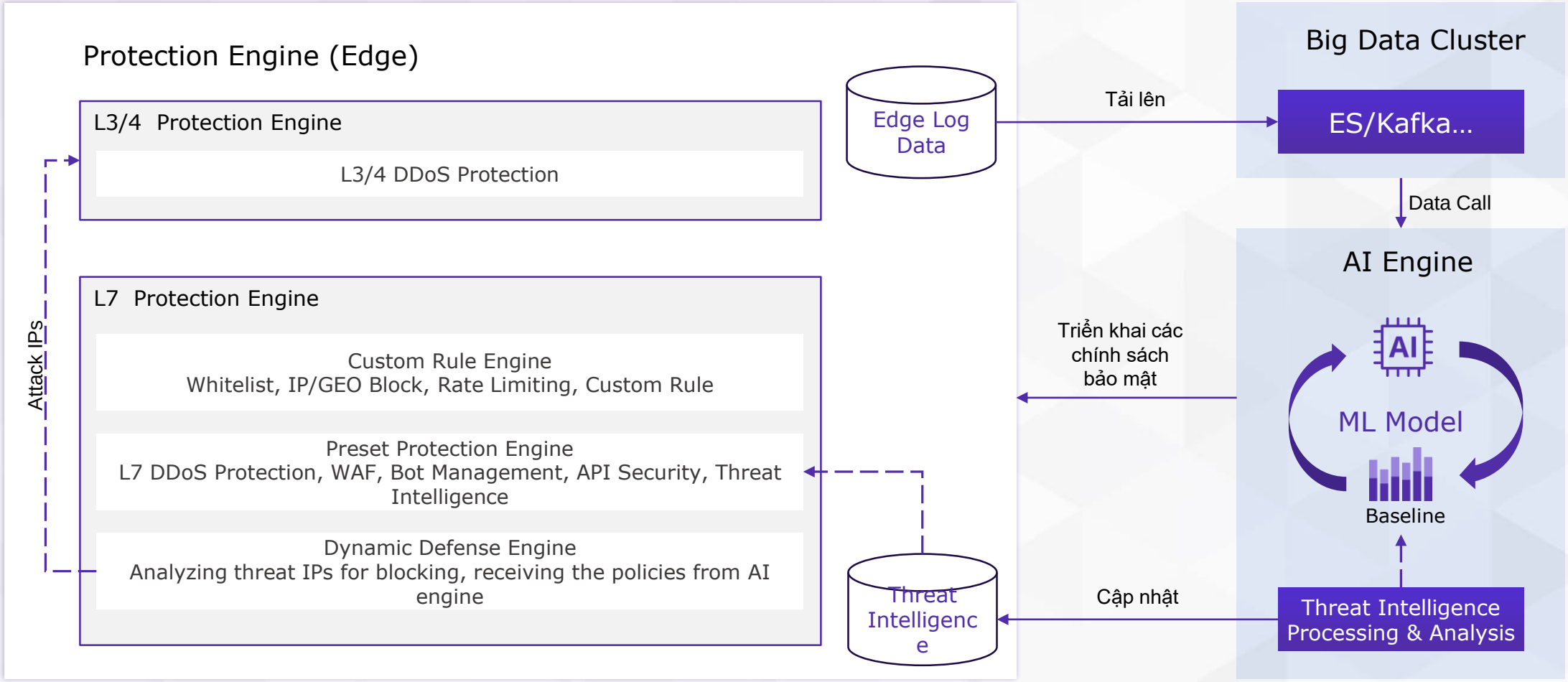
Phòng chống tấn công DDoS lớp 3/4 và lớp 7

Tiết kiệm chi phí

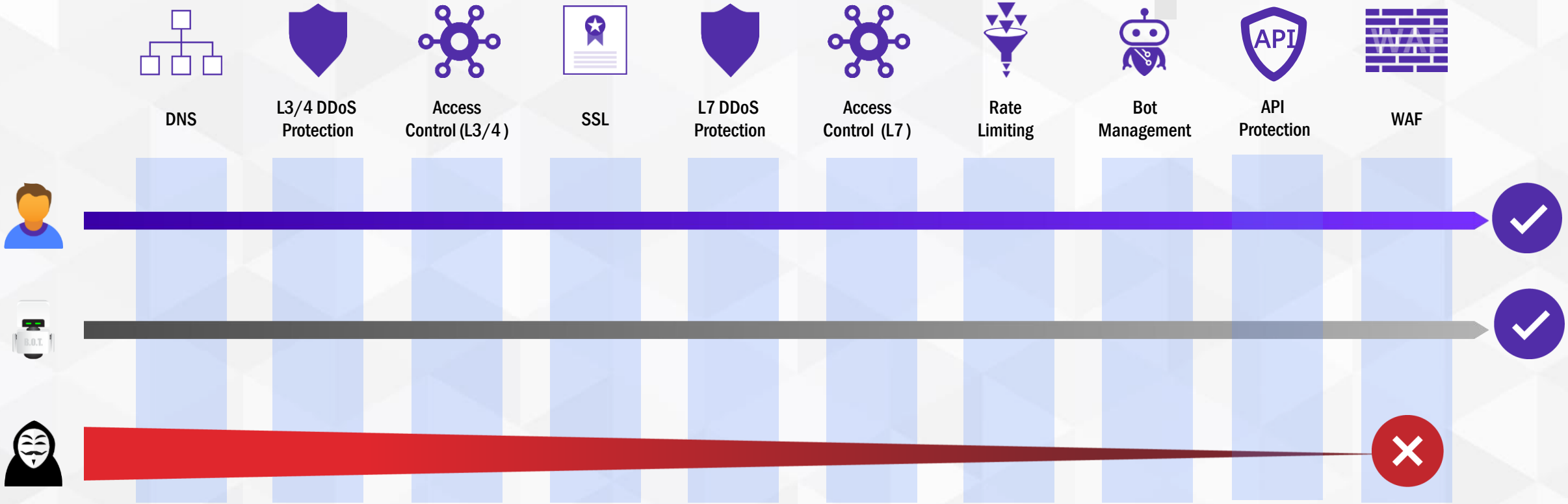
-50%

Vận hành đơn giản
Quản lý dễ dàng
An toàn, hiệu quả

Công nghệ bảo vệ đa tác vụ



Kết Hợp Nhiều Lớp Công Nghệ Bảo Mật Chạy 24/7

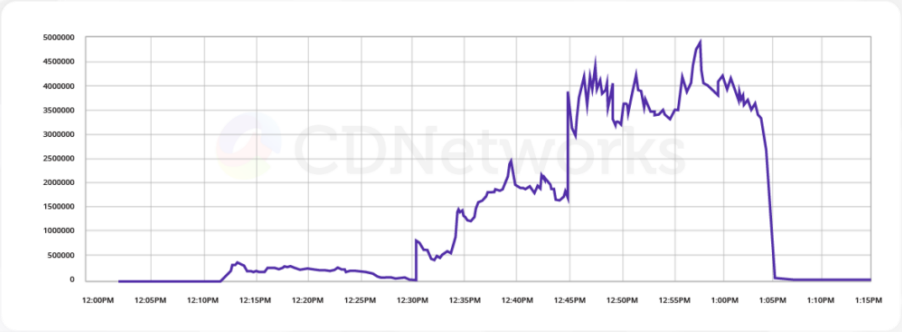


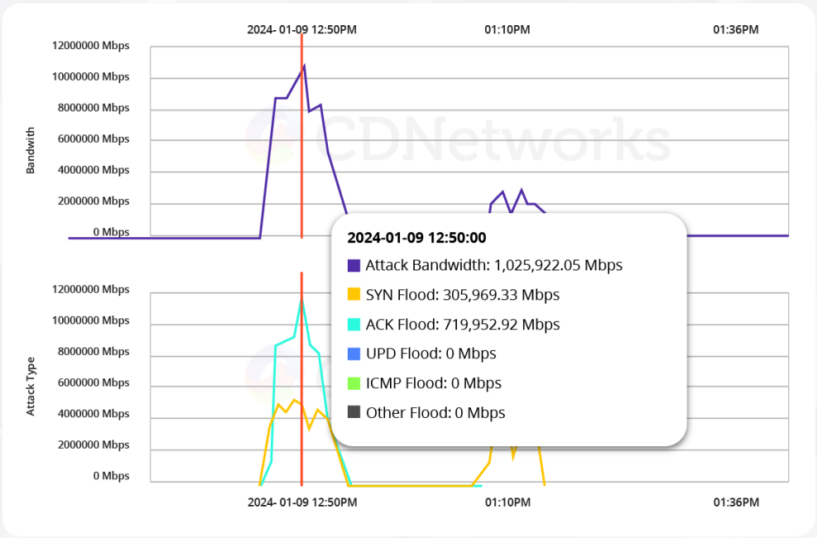
Phòng chống tấn công DDoS lớp 3/4

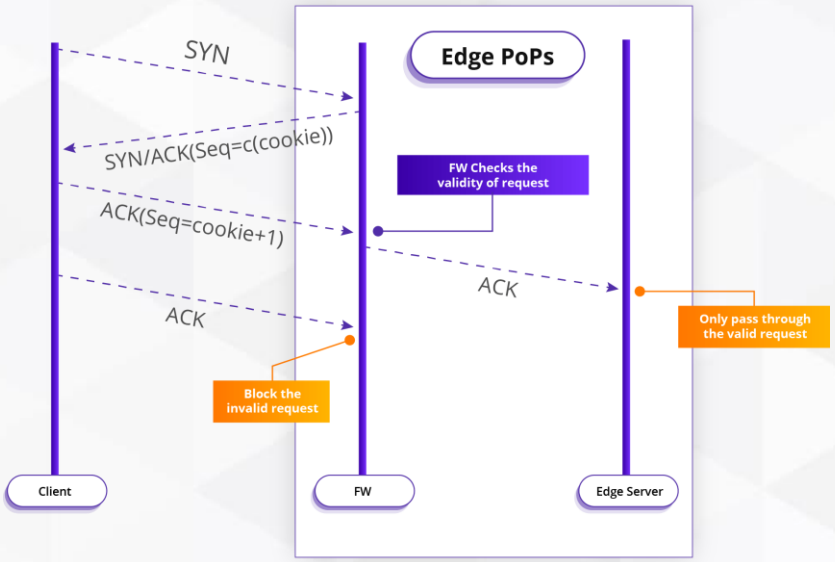
Phòng chống, ngăn chặn và giảm thiểu các loại hình tấn công từ chối dịch vụ DDoS ở lớp 3/4 như là:

- ✓ SYN Flood
- ✓ ACK Flood
- ✓ UDP Flood
- ✓ ICMP Flood
- ✓ Reflected Attack
- ✓ Amplified Attack

… …







Kiến trúc phòng chống tấn công DDoS

Phòng chống tấn công DDoS lớp 7

Năng lực phòng chống

Có khả năng phòng chống 1 billion RPS

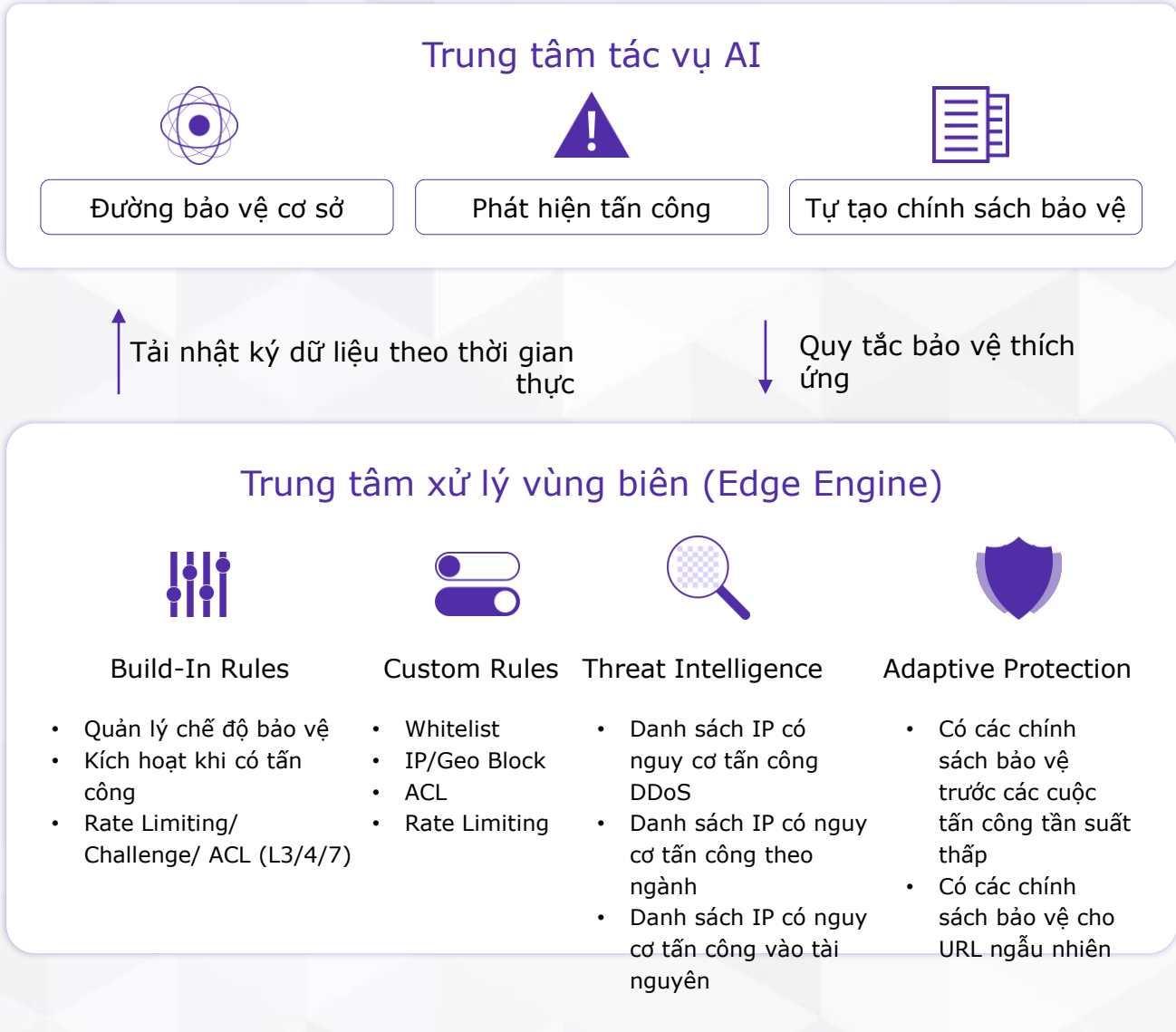
- Giảm thiểu các loại hình tấn công HTTP/S floods (GET/POST), SlowLoris, .v.v.

Kích hoạt dịch vụ bằng 1 click chuột

- Kích hoạt các tính năng bảo mật chỉ bằng một cái click chuột mà không phải chuyển đổi giao diện.

Bảo vệ thích ứng

- Cập nhật đường cơ sở động dựa theo phân tích lưu lượng truy cập và tấn công thực tế.
- Tự động tạo các quy tắc bảo vệ để phòng chống tấn công
- Là lớp phát hiện tấn công thứ 2



Web Application Firewall

Có nhiều năm kinh nghiệm cung cấp dịch vụ bảo mật

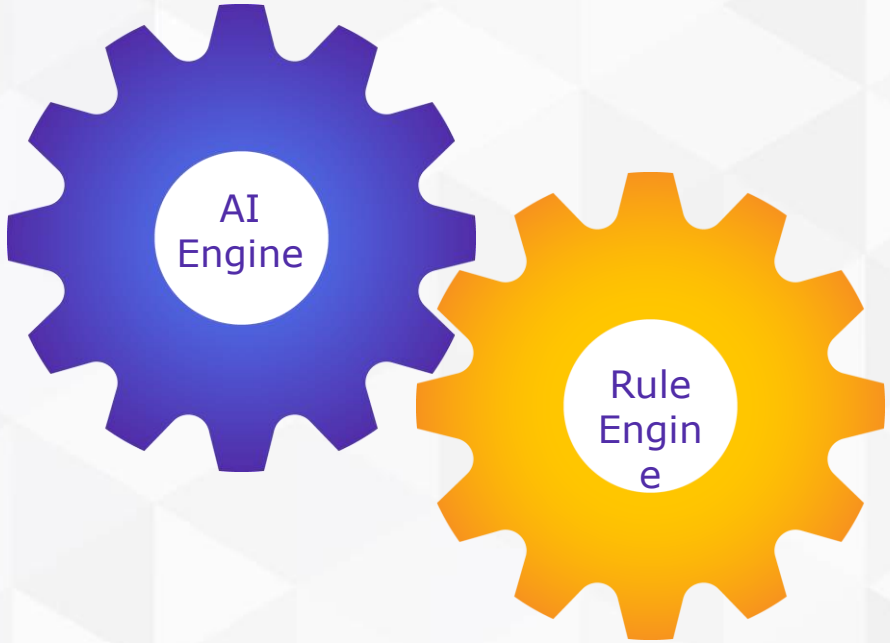
- Chống tấn công Top 10 lỗ hổng bảo mật theo OWASP
- Trên 90% các tên miền WAF chạy ở chế độ chặn
- Phát triển dịch vụ WAF bao gồm các tập lệnh (rulesets) với các mẫu tấn tấn được tích hợp sẵn.

Bản vá ảo cho các cuộc tấn công 0-day

Đội ngũ chuyên gia bảo mật luôn theo dõi, phân tích và cập nhật các mẫu tấn công 0-day mới nhất, các bản vá được tạo ra ngay khi lỗ hổng đó được công bố

Phân tích thông minh

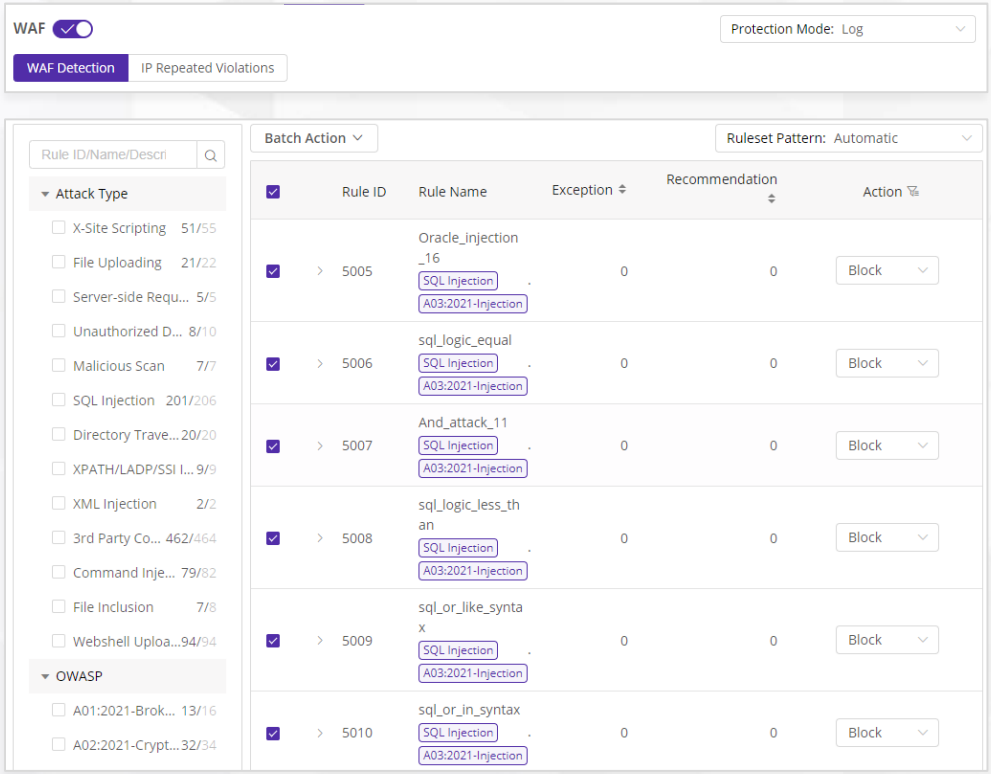
Sử dụng công nghệ AI trong việc phân tích các hành vi truy cập của người dùng cuối, tự động tạo ra các qui tắc ngăn chặn ngoại lệ để giảm thiểu việc bắt lỗi nhầm.

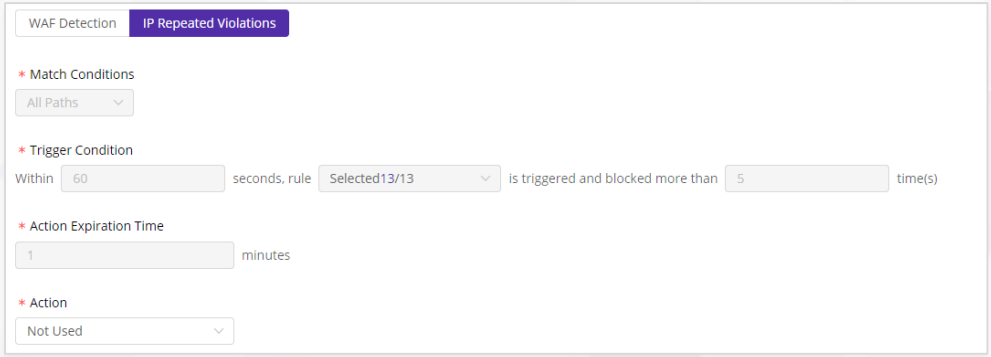


Web Application Firewall

Rule Engine

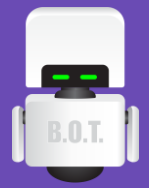
- Hơn 1000 các mẫu tấn công chống khai thác các lỗ hổng 0-day/N-day
- Hàng trăm mẫu qui tắc WAF dùng để chống lại các loại tấn công như SQLi, XSS, Xpath và loại tấn công ở lớp ứng dụng thuộc **Top 10 OWASP**.
- Chế độ tự động cập nhật các tập lệnh mới nhất và tự động triển khai các đề xuất xử lý ngoại lệ.
- Chặn IP tấn công chặn các IP vi phạm các qui tắc WAF nhiều lần.
- Phát hiện chèn mã độc prevent ngăn chặn việc chèn các loại mã hoặc phần mềm độc hại như Trojans.
- Nhiều chế độ xử lý như là giám sát, chặn, không sử dụng v.v.





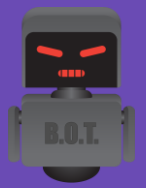
Quản Lý Bot

Quản lý Bot Tốt



- Whitelist cho những Bot tốt
- Tùy chỉnh nhận diện các Bot tốt
- Thay đổi các chế độ bảo vệ như là bỏ qua, giám sát, chặn hoặc giới hạn truy cập.v.v.

Quản lý Bot Độc hại



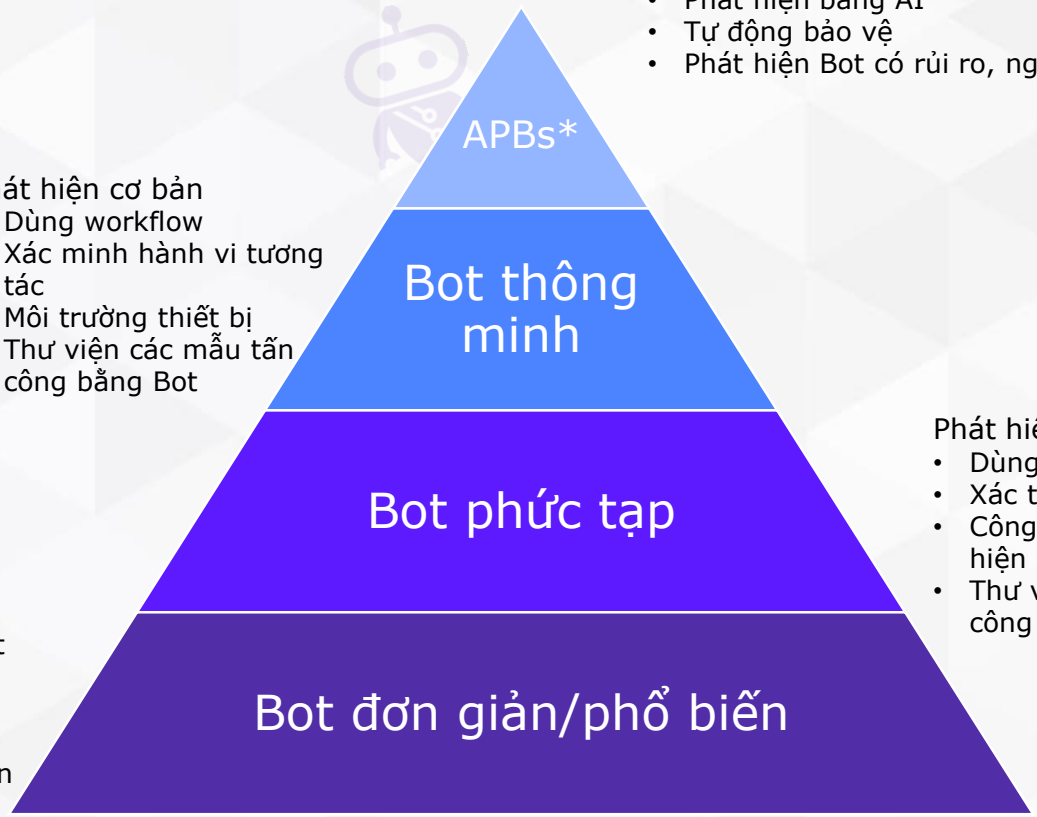
- Chặn các Bot vi phạm truy cập nhiều lần
- Thay đổi các chế độ bảo vệ như chặn, đánh dấu, giám sát, captcha .v.v.

Quản lý Bot

Phát hiện và ngăn chặn nhiều loại Bot bằng nhiều chính sách bảo mật khác nhau

Các tình huống bảo vệ

- ✓ Dò quét nội dung
- ✓ Mua đầu cơ
- ✓ Brute Force
- ✓ Chiếm đoạt tài khoản
- ✓ Nhồi nhét thông tin xác thực
- ✓ Gian lận đăng ký
- ✓ Gian lận hàng tồn kho
- ✓ và nhiều tình huống khác



Phát hiện nâng cao (Intelligent Risk Detection)
- Phát hiện bằng AI
- Tự động bảo vệ
- Phát hiện Bot có rủi ro, nguy cơ tấn công cao

Phát hiện cơ bản
- Dùng workflow
- Xác minh hành vi tương tác
- Môi trường thiết bị
- Thư viện các mẫu tấn công bằng Bot

Phát hiện cơ bản
- Dùng mã Captcha
- Xác thực bằng token
- Công vụ tự động phát hiện
- Thư viện các mẫu tấn công bằng Bot

Phát hiện cơ bản
- Xác minh trình duyệt
- Thư việc Bot tốt/Bot xấu
- Bot tùy biến
- Thư viện các mẫu tấn công bằng Bot

*APBs: Advance Persistence Bots

Bảo mật API

Giải pháp bảo vệ API dựa trên quy trình "Phát hiện-Khai báo-Bảo vệ" tạo thành một vòng bảo mật API khép kín.

Bảo Vệ API

Quản lý dễ dàng và hiệu quả

Dễ dàng quản lý và bảo vệ các API hiện có. Phát hiện các API chưa được khai báo và giúp khách hàng tránh khỏi các cuộc tấn công bằng cách khai thác các lỗ hổng API theo thời gian thực.

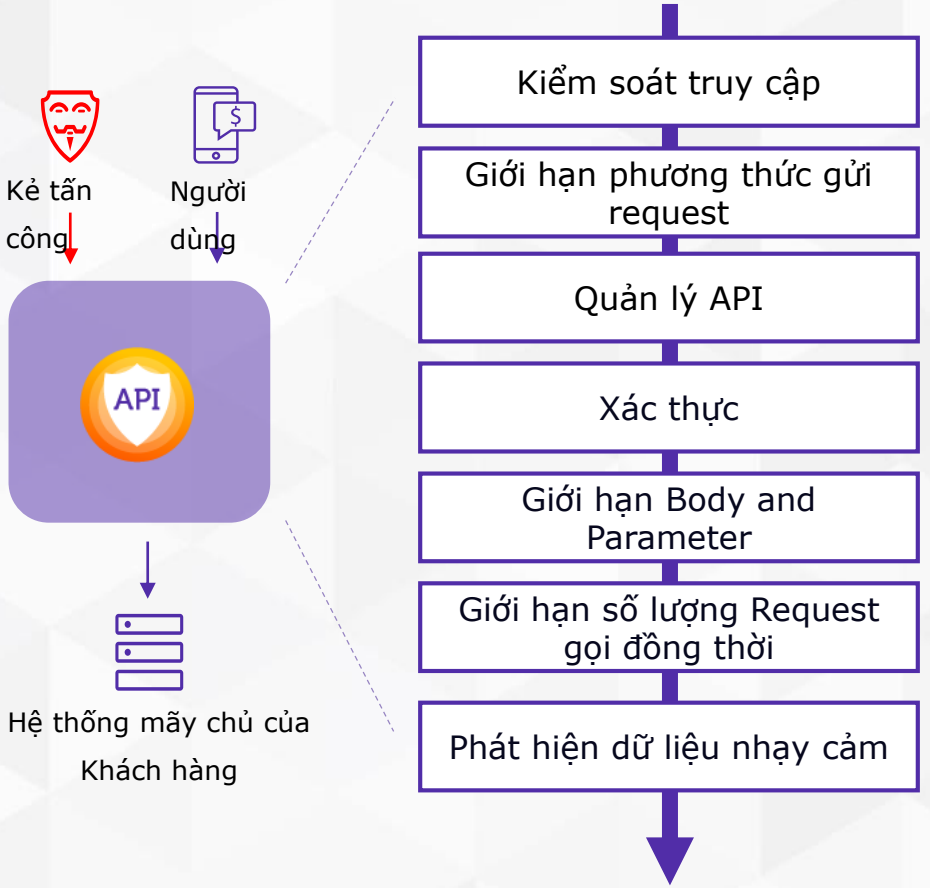
Bảo vệ đa lớp

Sử dụng nhiều tiến trình bảo vệ chạy đồng thời để phát hiện và ngăn chặn các cuộc tấn công API trước khi được gọi đến Hệ thống máy chủ.

Kiểm soát lưu lượng

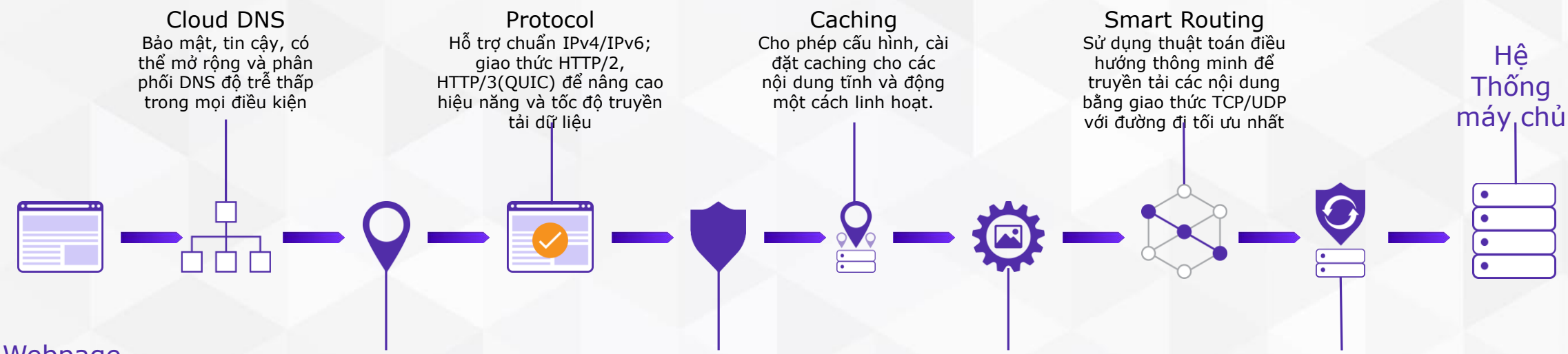
Hỗ trợ 2 phương thức kiểm soát lưu lượng:

- Giới hạn API Request: Kiểm soát lưu lượng trong một khoảng thời gian định trước.
- Giới hạn số lượng Request gọi đồng thời: Kiểm soát lưu lượng truy cập toàn cầu cho từng API.



Tăng Hiệu Năng Ứng Dụng Web

Giải Pháp Tăng Tốc Web



Webpage

Cloud DNS
Bảo mật, tin cậy, có thể mở rộng và phân phối DNS độ trễ thấp trong mọi điều kiện

NGB Scheduling
Sử dụng thuật toán cân bằng tải để tối ưu hiệu suất truy cập, cũng như giảm thời gian tải trang cho người dùng cuối

Protocol
Hỗ trợ chuẩn IPv4/IPv6; giao thức HTTP/2, HTTP/3(QUIC) để nâng cao hiệu năng và tốc độ truyền tải dữ liệu

Security
Encrypt Mã hóa toàn bộ dữ liệu truyền tải, nhằm đảm bảo an toàn và bảo mật thông tin bằng cách sử dụng giao thức mã hóa TLS

Caching
Cho phép cấu hình, cài đặt caching cho các nội dung tĩnh và động một cách linh hoạt.

Image Processing
Xử lý và hỗ trợ thay đổi định dạng, kích thước hình ảnh, nhằm giảm kích thước tệp tin hình ảnh mà vẫn đảm bảo chất lượng

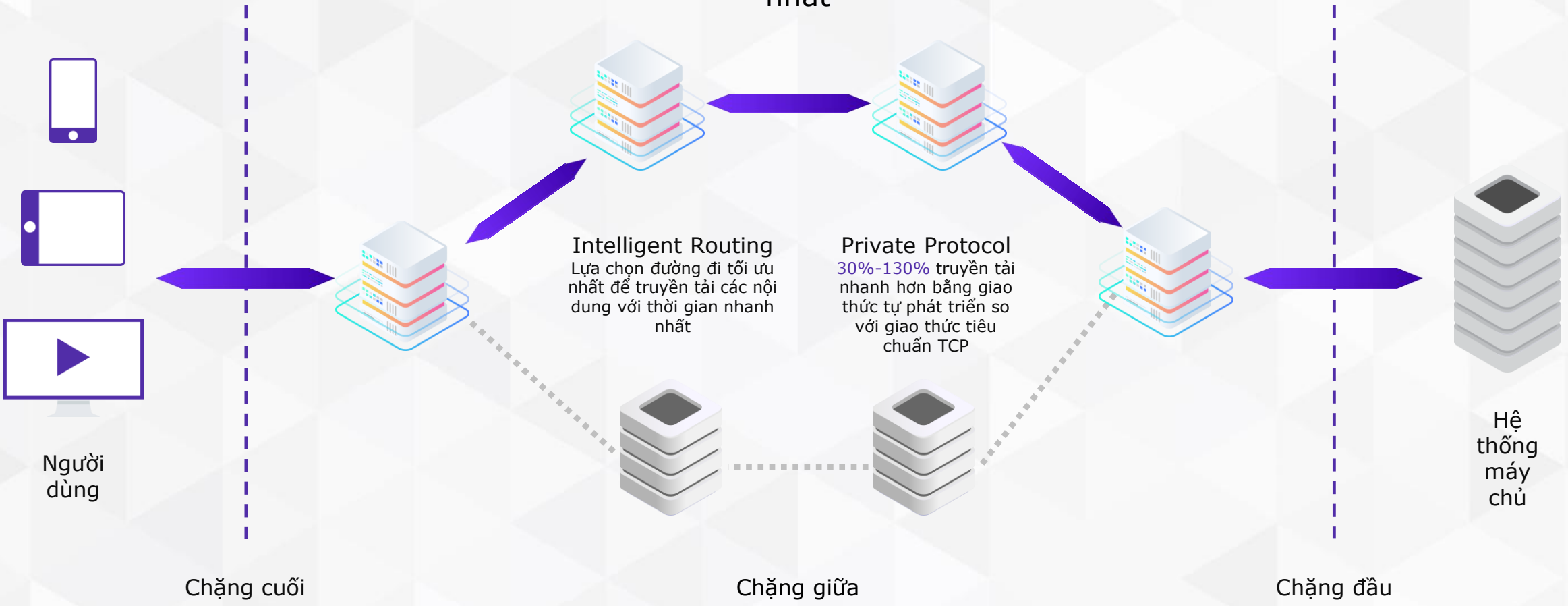
Smart Routing
Sử dụng thuật toán điều hướng thông minh để truyền tải các nội dung bằng giao thức TCP/UDP với đường đi tối ưu nhất

Origin offloading
Kết nối và giám sát hệ thống máy chủ, đồng thời giúp cho hệ thống máy chủ không bị quá tải

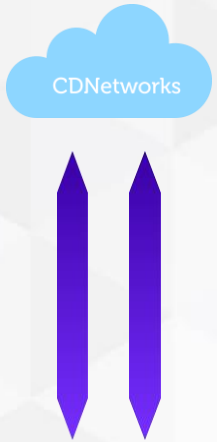
Hệ Thống máy chủ

Điều Hướng Thông Minh - Smart Routing

CDNetworks truyền tải dữ liệu qua giao thức TCP/UDP bằng thuật toán Điều hướng thông minh với đường đi tối ưu nhất



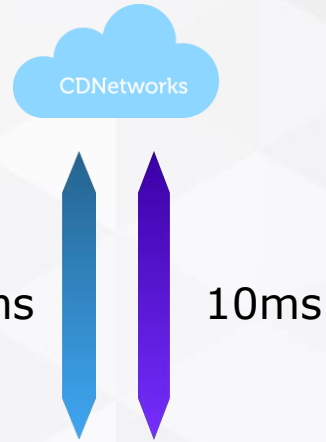
Giảm Tải Hệ Thống Máy Chủ



Connection Reuse

Tối thiểu hóa độ trễ khi gọi về hệ thống máy chủ bằng các kết nối TCP

Origi
n

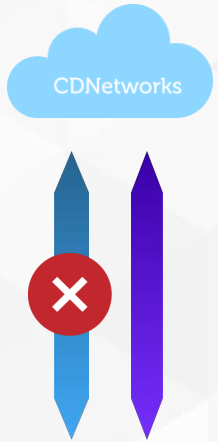


Origin Probe

Chọn hệ thống máy chủ có hiệu năng tốt nhất để truy cập và lấy dữ liệu.

Origin
1

Origin
2



Monitoring

Tự động giám sát, cảnh báo khi kết nối đến hệ thống máy chủ bị lỗi

Master
Origin

Slave
Origin

Tuân thủ và Chứng nhận Bảo mật

ISO/IEC 27001

ISO/IEC 27001: 2013 là chứng nhận bảo mật thông tin toàn ngành, tập trung vào việc triển khai Hệ thống Quản lý Bảo mật Thông tin (ISMS) và các quy trình quản lý rủi ro bảo mật.

PCI DSS COMPLIANT

The Payment Card Industry Data Security Standard (PCI DSS) là một tiêu chuẩn an ninh thông tin bắt buộc dành cho các doanh nghiệp lưu trữ, truyền tải và xử lý thẻ thanh toán. Tiêu chuẩn PCI DSS được phát triển nhằm hỗ trợ các tổ chức thanh toán thẻ bảo vệ dữ liệu của khách hàng, chống lại việc xâm nhập và sử dụng dữ liệu khi chưa được phép.

정보보호 관리체계 인증 ISMS Information Security Management System

ISMS là hệ thống quản lý an toàn thông tin xác định và quản lý các biện pháp kiểm soát mà tổ chức cần thực hiện để đảm bảo rằng tổ chức đang bảo vệ một cách hợp lý tính bí mật, tính sẵn có và tính toàn vẹn của tài sản khỏi các mối đe dọa và lỗ hổng bảo mật.

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations

A SOC 2 là báo cáo đánh giá cho các tổ chức dịch vụ là đáng tin cậy, được thiết kế nhằm đảm bảo rằng các nhà cung cấp dịch vụ quản lý dữ liệu một cách an toàn để bảo vệ lợi ích của tổ chức và quyền riêng tư của khách hàng.

Chính sách KINH DOANH

1. Dịch vụ Chống tấn công DDoS cho Web

- Phát hiện và Ngăn chặn Tấn công DdoS
- Giảm thiểu độ trễ (Latency)
- Bảo vệ trong thời gian thực
- Hỗ trợ tự động và thủ công

STT	Gói dịch vụ	Giá bán (vnđ)/tháng	Mô tả
Gói 1	500GB	4,940,000	Bao gồm các tính năng Phòng chống tấn công DDOS: Advance Access Control, Rate Limiting, L3/L4/L7 DDOS Mitigation, Preset Protection Policies, Log and incident investigation tools basic, Deploy history...
Gói 2	1000GB	9,880,000	
Gói 3	2000GB	19,760,000	
Gói 4	3000GB	29,640,000	
Gói 5	5000GB	49,400,000	
Gói 6	Tùy chỉnh theo yêu cầu khách hàng		

2. Dịch vụ tường lửa cho ứng dụng web

- Bảo vệ chống tấn công OWASP Top 10
- Kiểm tra và lọc lưu lượng HTTP/HTTPS
- Giám sát và cảnh báo thời gian thực
- Tối ưu hóa hiệu suất (Caching)

STT	Gói dịch vụ	Giá bán (vnđ)/tháng	Mô tả
Gói 1	500GB	7,410,000	- Bao gồm các tính năng Phòng chống tấn công DDOS: Advance Access Control, Rate Limiting, L3/L4/L7 DDOS Mitigation, Preset Protection Policies, Log and incident investigation tools basic, Deploy history... - Bao gồm các tính năng bảo vệ WAF: Advance Access Control, Rate Limiting, IP Repeated Violations, HTTP Protocal validation, Built-in WAF Rules, OWASP Core Rulesets, Zero day protection, Rule template management, WAF Dashboard, WAF intelligent Analysis Service, Custom WAF Rules, Coinhive Prevention, Webshell Access Detection on Origin, Adware Insertion Prevention,...
Gói 2	1000GB	14,820,000	
Gói 3	2000GB	29,640,000	
Gói 4	3000GB	44,460,000	
Gói 5	5000GB	74,100,000	
Gói 6	Tùy chỉnh theo yêu cầu khách hàng		

3. Dịch vụ quản lý BOT

- Phát hiện BOT tự động
- Chặn BOT xấu và gian lận
- Phân loại BOT (Human vs Bot)

STT	Gói dịch vụ	Giá bán (vnđ)/Tháng	Mô tả
Gói 1	500GB	3,705,000	Bao gồm các tính năng chống BOT: BOT Intelligence, BOT Detection, Fingerprint Analisys, Advance detections, …
Gói 2	1000GB	7,410,000	
Gói 3	2000GB	14,820,000	
Gói 4	3000GB	22,230,000	
Gói 5	5000GB	37,050,000	
Gói 6	Tùy chỉnh theo yêu cầu khách hàng		

4. Dịch vụ tường lửa cho API

- Phát hiện và ngăn chặn tấn công API
- Phát hiện API Vulnerabilities
- Bảo vệ API bằng phương thức kiểm tra xác thực mạnh
- Giám sát và cảnh báo thời gian thực

STT	Gói dịch vụ	Giá bán (vnđ)/tháng	Mô tả
Gói 1	500GB	2,470,000	- Bao gồm các tính năng bảo vệ API: API inventory, API Discovery, API Authentification, API Parameter Compliance Detection, …
Gói 2	1000GB	4,940,000	
Gói 3	2000GB	9,880,000	
Gói 4	3000GB	14,820,000	
Gói 5	5000GB	24,700,000	
Gói 6	Tùy chỉnh theo yêu cầu khách hàng		

5. CDN Add-on

STT	Gói dịch vụ	Giá bán (vnđ)/tháng	Mô tả
Gói 1	Không cam kết hoặc dưới 1000TB	300,000	- Bao gồm các tính năng tăng tốc ứng dụng: Intelligent Routing, WebSocket, HTTP 2.0, IPV6 Services, QUIC, TLS 1.3, HTTPS, Antu Hotlinking, Port Customisation, Image porocessing…
Gói 2	1000TB<MG<5000TB	228,000	
Gói 3	5000TB<MG<10000TB	190,000	
Gói 4	MG>10000TB	152,000	
Gói 6	Tùy chỉnh theo yêu cầu khách hàng		

Bao gồm các tính năng tăng tốc ứng dụng: Intelligent Routing, WebSocket, HTTP 2.0, IPV6 Services, QUIC, TLS 1.3, HTTPS, Antu Hotlinking, Port Customisation, Image porocessing…

CẢM ƠN!