VNIS
Vnetwork Internet Security

Bảo mật và tăng tốc cho Web/App/API

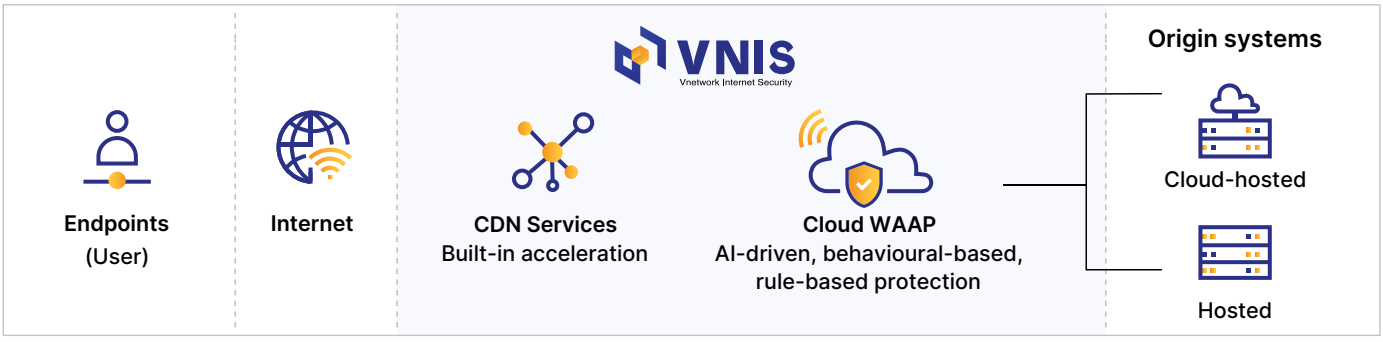
Giải pháp **VNIS WAAP** bảo mật được kiến tạo từ AI – nơi AI không chỉ là công cụ hỗ trợ, mà đóng vai trò trung tâm trong việc **xây dựng giải pháp, dự báo, nhận diện** và **phòng chống các cuộc tấn công mạng** ngày càng tinh vi.

VỚI VNIS DOANH NGHIỆP CÓ THỂ?

- **Bảo vệ Web/App/API khỏi các tấn công theo thời gian thực:** DDoS layer 3/4/7, bot attack, khai thác lỗ hổng bảo mật, zero-day, crawlers/malware...
- **Phát hiện và ngăn chặn mối đe dọa** ngay từ giai đoạn đầu mà không làm ảnh hưởng đến trải nghiệm người dùng và hiệu suất hệ thống.
- **Duy trì hiệu suất vượt trội,** kể cả trong những tình huống tải lưu lượng truy cập tăng cao hoặc tấn công có chủ đích.

Mô hình hoạt động

VNIS ở giữa người dùng cuối và origin systems với 2 layer chính là CDN và Cloud WAAP



Tổng quan tính năng và công nghệ

AI được tích hợp trong các tính năng cốt lõi mang lại hiệu suất vượt trội cho hệ thống

Bảo vệ chủ động

- **AI-WAF:** Chặn các cuộc tấn công tinh vi theo thời gian thực, đảm bảo website luôn hoạt động ổn định.
- **API protection:** Ngăn chặn truy cập trái phép và rò rỉ dữ liệu.
- **Bot management:** Ngăn hành vi scraping, fraud attempt và tấn công chiếm đoạt tài khoản.

Ứng dụng Threat Intelligence

- **Business threat awareness:** Phân tích hành vi để phát hiện giả mạo và hình thức tấn công mới.
- **Programmable mitigation:** Tự động triển khai biện pháp phòng vệ trước khi mối đe dọa lan rộng.

Tối ưu hiệu suất

- **DDoS mitigation:** Đảm bảo hoạt động ổn định ngay cả khi bị tấn công.
- **Content acceleration:** Tăng tốc tải trang, đảm bảo hiệu suất ngay cả khi lưu lượng truy cập tăng cao.

Ứng phó khẩn cấp

- **Emergency mitigation:** Kích hoạt chế độ phòng vệ khẩn cấp và read-only để ngăn chặn mối đe dọa ngay lập tức.

Công nghệ

AI-Driven Awareness

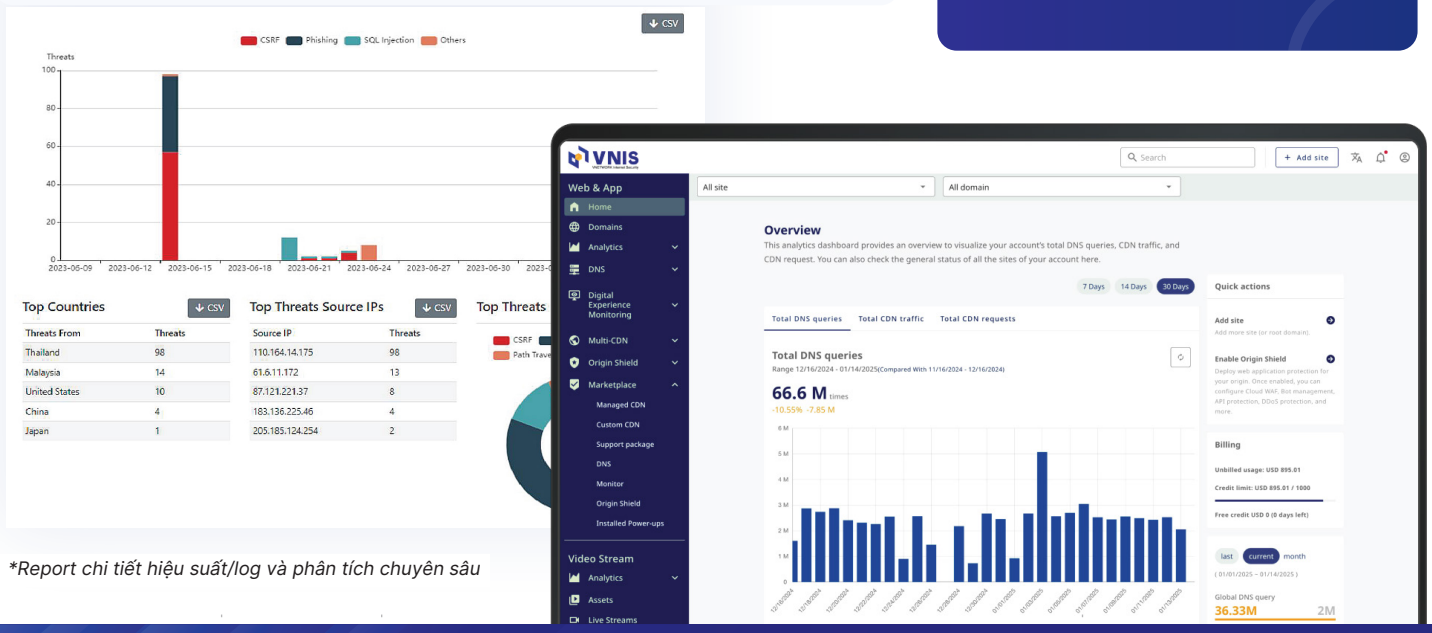
Phát hiện mối đe dọa bằng cách phân tích ngữ cảnh và hành vi tấn công

Rule-Based

Áp dụng cơ chế kiểm soát signature-based và policy-based để ngăn chặn các mối đe dọa đã biết và mới nổi

Behaviour-Based

Phân tích hành vi người dùng để phát hiện tấn công tự động



*Report chi tiết hiệu suất/log và phân tích chuyên sâu

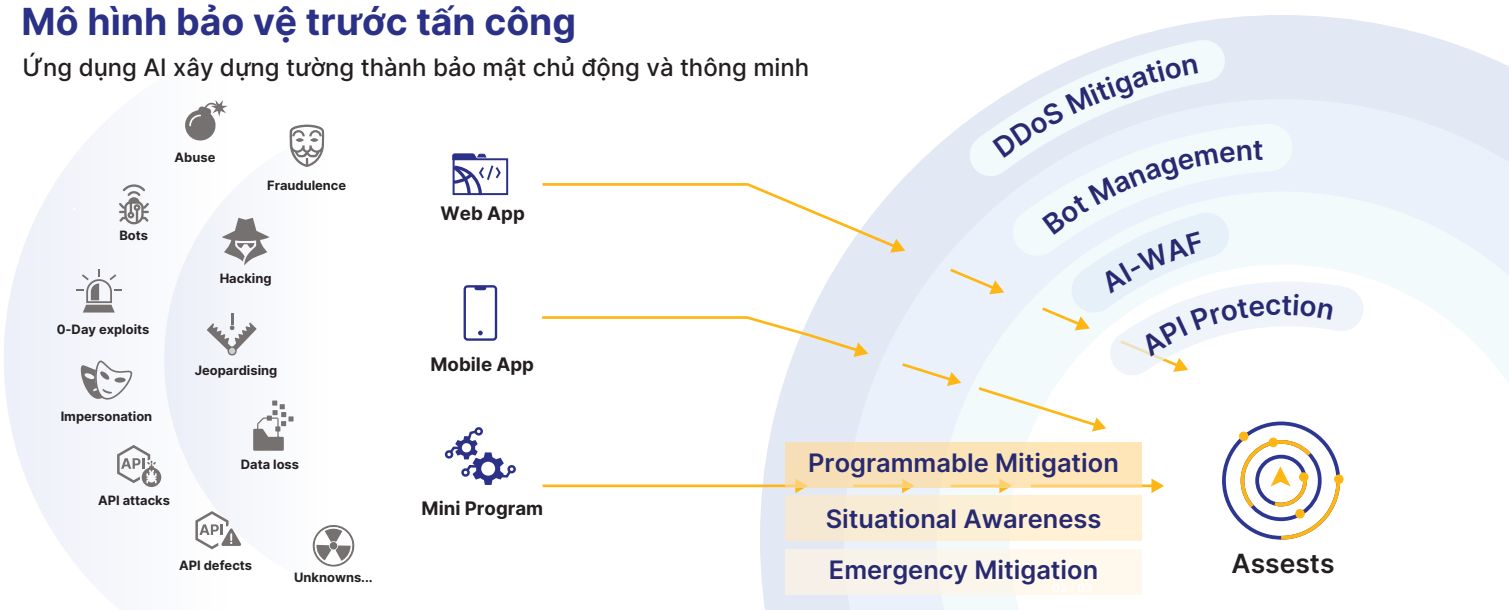
Chi tiết tính năng cốt lõi

Next-gen WAF với đa dạng tính năng phòng chống toàn diện cho Web/App/API

Tính năng cốt lõi	Cách hoạt động	Tác động	Bảo vệ khỏi tấn công
AI-WAF	Ngăn chặn các mối đe dọa web tinh vi theo thời gian thực và cảnh báo liên tục	Phát hiện tấn công bằng AI, phân tích ngữ cảnh, quy tắc động (rule engine), chống các thay đổi trái phép	Tấn công Injection, Brute Force, Defacement, OWASP Top 10
API Protection	Phân tích hoạt động API để ngăn chặn lạm dụng, truy cập trái phép và rò rỉ dữ liệu	Xác thực lược đồ API, triển khai DLP, giám sát trình tự giao tiếp	Lạm dụng API, thất thoát dữ liệu nhạy cảm, khai thác lỗi logic nghiệp vụ
Bot Management	Chặn cào dữ liệu, tấn công tự động và chiếm đoạt tài khoản	Nhận diện dấu vân tay (fingerprinting), rủi ro tiềm ẩn, CAPTCHA, xác thực trình duyệt	Nhồi nhét thông tin đăng nhập, cào dữ liệu, đăng ký giả, tấn công tự động hóa
Business Threat Awareness	Phát hiện các mối đe dọa mới nổi như giả mạo và gian lận qua phân tích hành vi	Đánh giá và cảnh báo mối đe dọa, theo dõi hành vi, phát hiện mẫu gian lận	Giả mạo danh tính, chiến dịch lừa đảo, xu hướng đe dọa mới
Programmable Mitigation	Tự động hóa phòng thủ dựa trên hành vi traffic và logic nghiệp vụ	Quy tắc tùy chỉnh, progressive overload, kiểm soát luồng	Lạm dụng thanh toán, khai thác logic, can thiệp giao dịch
DDoS Mitigation	Duy trì tốc độ và tính liên tục ngay cả trong các cuộc tấn công	Giới hạn tốc độ, bộ lọc dựa trên hành vi, chống đột biến lưu lượng độc hại	Tấn công DDoS layer 3/4/7, lãng phí tài nguyên và bùng phát lưu lượng
Content Acceleration	Nâng cao hiệu suất Web/App toàn cầu, ngay cả khi lưu lượng tăng đột biến	Lưu trữ biên, cân bằng tải CDN, tự động hóa chứng chỉ SSL/TLS, hỗ trợ HTTP/2 & HTTP/3	Tốc độ trang chậm, độ trễ nội dung cao
Emergency Mitigation	Kích hoạt phản ứng tức thời trong các cuộc tấn công nghiêm trọng hoặc sự kiện trực tiếp	Phòng vệ khẩn cấp - ngắt kết nối, chặn theo khu vực, static mode, read-only controls	Sự kiện bất ngờ, tăng đột biến lưu lượng

Mô hình bảo vệ trước tấn công

Ứng dụng AI xây dựng tường thành bảo mật chủ động và thông minh



Các gói dịch vụ

Gói dịch vụ linh hoạt, tối ưu chi phí và đảm bảo tính an toàn bảo mật

THÔNG TIN GÓI/THÁNG Giá	BASIC Chỉ từ 5,200,000đ	Đề xuất ADVANCE Chỉ từ 19,500,000đ	ENTERPRISE
FQDN* bảo vệ *Fully Qualified Domain Name*	2	2	Tuỳ chỉnh
Traffic	1TB	2TB	
Peak RPS (hoặc Tổng request)	100 RPS (5Triệu)	200 RPS (10 triệu)	
WAAP			
AI-WAF	✓	✓	✓
DDoS Mitigation	✓	✓	✓
Bot Management	–	✓	✓
API Protection	–	✓	✓
Emergency Mitigation	✓	✓	✓
Programmable Mitigation	–	✓	✓
Business Threat Awareness	–	✓	✓
Behavioral Analytics	✓	✓	✓
CDN			
Content Acceleration	✓	✓	✓
Content Caching	✓	✓	✓
Global Load Balance	✓	✓	✓
Certificate Management	✓	✓	✓
Multi-CDN	–	✓	✓
DEM (Digital Experience Management)	✓	✓	✓
Administration & API			
Multi-user Administrative Access	–	✓	✓
Role-based Access Control	✓	✓	✓
Single Sign-On (SSO) Support	✓	✓	✓
Open API	✓	✓	✓
Consultancy			
Solution integration and onboarding	✓	✓	✓
Portal administration and Web Security Fundamentals training	✓	✓	✓
Web application scanning report (if allowed)	✓	✓	✓
DNS (Domain Name System)	–	✓	✓
SOC	✓	✓	✓

Thông tin liên hệ:

+84 (028) 7306 8789

contact@vnetwork.vn

Quét mã QR để tìm hiểu thêm về các giải pháp an ninh mạng của chúng tôi hoặc truy cập **www.vnetwork.vn**