Cloudrity

CLOUDRITY.COM.VN

viettel security

Datasheet

***Cloudrity** - Dịch vụ bảo vệ website và ứng dụng trực tuyến*

Cloudrity

Là giải pháp bảo vệ toàn diện cho website và ứng dụng trực tuyến được triển khai dưới dạng dịch vụ trên nền tảng điện toán đám mây của Công ty An ninh mạng Viettel. Cloudrity được Viettel tự phát triển và tối ưu hóa để tăng cường hiệu suất và tính ổn định của sản phẩm nhằm đảm bảo đem lại dịch vụ bảo mật đáng tin cậy nhất, tối ưu nhất cho khách hàng.

Đảm bảo dịch vụ luôn sẵn sàng

Giảm thiểu ảnh hưởng khỏi các cuộc tấn công từ chối dịch vụ quy mô lớn từ tầng mạng đến tầng ứng dụng, giúp cho website và ứng dụng của khách hàng luôn sẵn sàng.

Bảo vệ dữ liệu, thông tin

Bảo vệ website và ứng dụng trước các cuộc tấn công khai thác lỗ hổng web như TOP10 OWASP, 1-day, 0-day với nguồn tri thức bảo mật từ các chuyên giabảo mật hàng đầu Việt Nam của Viettel, tránh việc mất thông tin nhạy cảm.

Pay-as-you-use

Chi phí linh hoạt, hợp lý theo mô hình điện toán đám mây, giúp khách hàng chỉ chi trả cho những gì cần dùng, không tốn chi phí cố định hàng tháng không cần thiết để duy trì dịch vụ

Phù hợp với mọi quy mô website và ứng dụng

Triển khai không cần lắp đặt, nhanh chóng, dễ dàng, tùy theo nhu cầu của khách hàng, không có bất cứ giới hạn nào về quy mô website và ứng dụng. Khách hàng có thể bắt đầu từ quy mô nhỏ và mở rộng theo sự tăng trưởng của website và ứng dụng gắn với sự tăng trưởng của hoạt động kinh doanh.

Hỗ trợ chuyên nghiệp, mọi lúc khi cần

Đội ngũ SOC (Security Operation Center) 24/7 đảm bảo xử lý kịp thời và chính xác các vấn đề ATTT xảy ra. Bên cạnh đó là đội ngũ CSKH chuyên nghiệp 24x7 qua nhiều phương thức hotline, email, chat, web ticket đảm bảo tiếp nhận và xử lý kịp thời mọi phản ánh.

KHÁCH HÀNG CỦA CLOUDRITY

THANH TRA CHÍNH PHỦ

Vietnam Airlines REACH FURTHER

THUẾ VIỆT NAM
TỔNG CỤC THUẾ - BỘ TÀI CHÍNH

EVN

BẢNG GIÁ

Vui lòng truy cập website hoặc liên hệ với chúng tôi

LIÊN HỆ | **+84 971 360 360**

cloudrity.com.vn

cskh_anm@viettel.com.vn

MÔ HÌNH GIẢI PHÁP

Cung cấp hệ thống bảo vệ 3 lớp

Lớp bảo vệ giảm thiểu tấn công DDOS tầng mạng (Mitigate DDoS Layer 3,4):

- Sử dụng hạ tầng mạng Viettel với năng lực cao để phân tán các lưu lượng tấn công DDoS tầng mạng, bảo vệ các máy chủ của khách hàng trước các cuộc tấn công với quy mô có thể lên tới vài chục Gbps.

Tường lửa bảo vệ các lỗ hổng Web (Web Application Firewall):

- Phát hiện, chặn lọc các dạng tấn công tinh vi nhằm vào lỗ hổng bảo mật Web. Được trang bị tập luật phát triển bởi chuyên gia Viettel, giúp phát hiện các dạng tấn công nhằm vào các lỗ hổng đã được công bố, và lỗ hổng chưa được công bố.

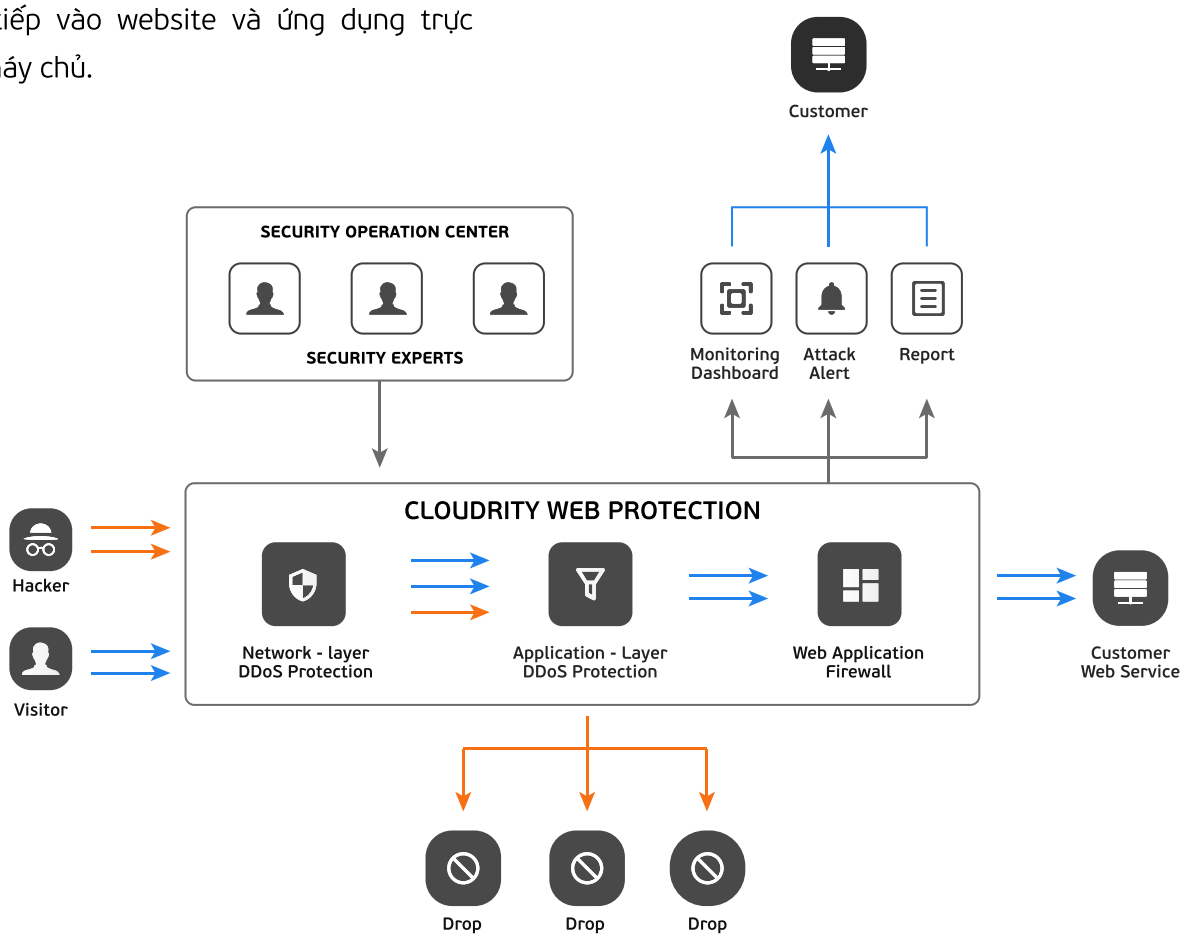
Lớp bảo vệ giảm thiểu tấn công DDOS tầng ứng dụng (Mitigate DDoS Layer 7):

- Phát hiện, chặn lọc các tấn công từ chối dịch vụ nhằm trực tiếp vào website và ứng dụng trực tuyến trên máy chủ.

Cung cấp dịch vụ hoàn thiện

- Core giải pháp trên mạng lưới/hạ tầng Viettel, triển khai theo mô hình multi-site với nhiều cụm dịch vụ
- Portal quản trị hoàn thiện dành cho khách hàng có thể tự cấu hình, giám sát, thống kê, theo dõi
- Đội ngũ Security Operation Center hoạt động 24/7/365 thực hiện giám sát, cảnh báo, phản ứng trước các cuộc tấn công mạng
- Đội ngũ chăm sóc khách hàng chuyên nghiệp, giàu kinh nghiệm, hoạt động 24/7/365

Mô hình giải pháp của Cloudrity



CLOUDRITY CUNG CẤP NHỮNG GÌ?

- Giảm thiểu tấn công từ chối dịch vụ lớp mạng (Layer 3,4) thông qua việc phát hiện các dấu hiệu bất thường dựa trên profile về lưu lượng thực tế của khách hàng. Bao gồm nhưng không giới hạn các kiểu tấn công sau: TCP SYN/ACK Flood, ICMP Flood, TCP Zero Window, Ping of Death, Teardrop, Volume-based (UDP, DNS, SMTP, Memcached, ...)

- Giảm thiểu tấn công từ chối dịch vụ lớp ứng dụng (Layer 7) với các kiểu tấn công phổ biến như, HTTP Flood, Slowloris, Slow Post, Sockstress, Scanner/Crawler, ... Cho phép người dùng cấu hình giới hạn băng thông, tần suất truy vấn theo từng IP cho từng tên miền

- Cho phép người dùng quản lý các IP, URI theo danh sách Whitelist/Blacklist

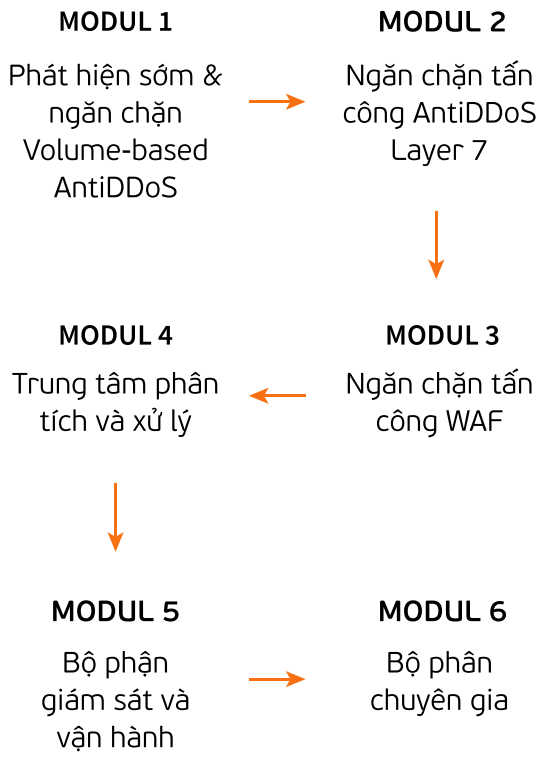
- Phát hiện và ngăn chặn các tấn công khai thác lỗ hổng web phổ biến như TOP10 OWASP, Cookie Poisoning, Brute Force Login, Directory Traversal, Session Hijacking, ... cũng như các lỗ hổng 1-day, 0-day được các kỹ sư Viettel nghiên cứu và phát hiện

- Hỗ trợ cho phép người dùng tự tối ưu và tùy chỉnh theo chuẩn ModeSecurity các tập luật được áp dụng cho riêng mình, giúp người dùng chủ động trong việc chặn/bỏ chặn các lỗ hổng web

- Hỗ trợ giám sát và phân tích lưu lượng truy cập theo thời gian thực với nhiều tiêu chí khác nhau như lượng khách truy cập hiện tại, tỷ lệ khách quay lại, tỷ lệ khách rời đi, tỷ lệ truy cập theo vị trí, ... Tính năng này phục vụ cho các hoạt động Marketing và SEO của website/ứng dụng.

- Hỗ trợ gửi thông báo, cảnh báo khi xảy ra sự kiện tấn công tới người sử dụng qua nhiều kênh khác nhau gồm SMS, Email, Telegram

Mô hình hoạt động của hệ thống



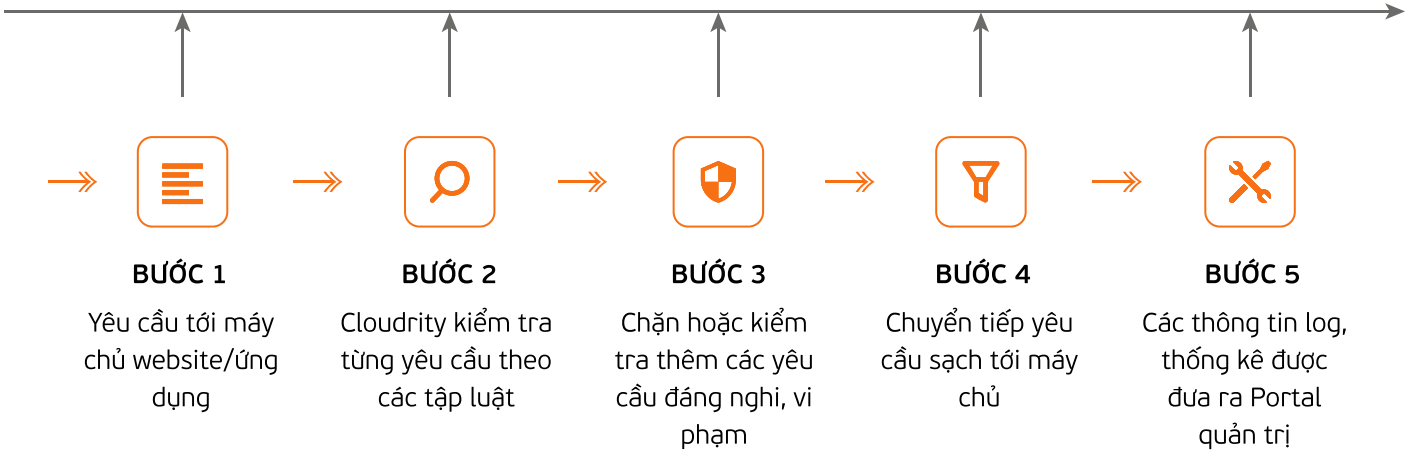
- Đảm bảo cơ chế bảo mật SSL toàn trình từ người dùng cuối tới máy chủ dịch vụ thông qua hỗ trợ TLS 1.3, cung cấp các chứng chỉ Free SSL tạm thời hoặc sử dụng các chứng chỉ SSL đã có.

- Tối ưu trải nghiệm người dùng thông qua việc hỗ trợ HTTP/2 cũng như cơ chế lưu cache các dữ liệu tĩnh, giúp cải thiện tốc độ và hiệu suất khi truy cập website và ứng dụng

- Cho phép người dùng quản lý các IP, URI theo danh sách Whitelist/Blacklist đã định nghĩa trước. Mọi truy cập từ Whitelist đều được thông qua, và ngược lại mọi truy cập từ Blacklist đều bị chặn

- Cho phép người dùng quản lý và phân loại giữa good bot (google, isp, ...) và bad bot (hacker). Mọi truy cập từ good bot đều được thông qua và các truy cập từ bad bot đều được chặn lại

CLOUDRITY HOẠT ĐỘNG NHƯ THẾ NÀO?



Bước 1

Mỗi một yêu cầu được gửi tới máy chủ website/ứng dụng của người dùng được thiết lập chuyển tiếp qua hệ thống Cloudrity. Tất cả các gói tin đều được đọc và phân tích dựa trên công nghệ phân tích gói tin sâu (DPI – Deep Packet Inspection).

Bước 2

Cloudrity kiểm tra từng yêu cầu dựa trên các tập luật được thiết lập mặc định bởi hệ thống hoặc được tùy chỉnh bởi người dùng, với các công nghệ Machine Learning, AI, Signature-based được áp dụng kết hợp với tập tri thức về các tấn công (TOP10 OWASP, 1-day, 0-day).

Bước 3

Bất cứ yêu cầu nào đáng nghi hay vi phạm các tập luật được thiết lập có thể được ngăn chặn, kiểm tra thêm, hoặc lưu log tuỳ theo thiết lập của người dùng.

Bước 4

Các lưu lượng sạch được chuyển tiếp đến các máy chủ website/ứng dụng. Các máy chủ website/ứng dụng này có thể là các máy chủ on-premise, on-cloud (public cloud, private cloud, hybrid cloud).

Bước 5

Cloudrity cung cấp giao diện cho phép người dùng linh hoạt xây dựng các tập luật thông qua các thao tác đơn giản.

viettel security