viettel
IDC

Datasheet
VIETTEL CLOUDRITY

Nhà cung cấp dịch vụ Trung tâm dữ liệu và Điện toán đám mây số 1 Việt Nam
Website: https://viettelidc.com.vn
Hotline: 1800 8088

Datasheet
VIETTEL CLOUDRITY

Tính năng nổi bật của Cloudrity

Chống tấn công DDoS tầng mạng (L4)

Tấn công DDoS (tấn công từ chối dịch vụ) sẽ đi đến hệ thống Cloudrity và được xử lý ngăn chặn bởi hệ thống/người vận hành trước khi đi đến server khách hàng.

Tường lửa ứng dụng WAF (Web Application Firewall)

Phát hiện, tự động ngăn chặn các request tấn công khai thác vào lỗ hổng của website (các kiểu tấn công thuộc TOP 10 OSWAP...)

Chống tấn công DDoS tầng ứng dụng (L7)

Phát hiện, tự động ngăn chặn tấn công thuộc các dạng HTTP Flood, Slow attack (Slow POST, Slow loris); ngăn chặn bot request đến website với cookie, captcha challenge.

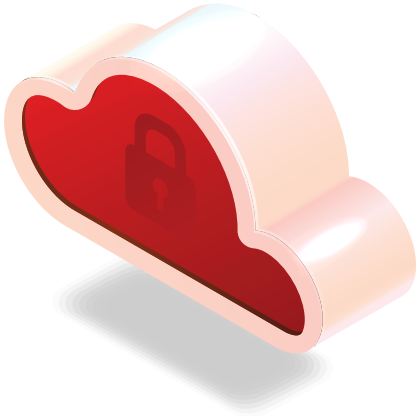
Nguy cơ an ninh mạng

Với tình hình COVID-19 vẫn diễn ra vô cùng phức tạp, kéo theo các nhu cầu chuyển đổi số mạnh mẽ, các tổ chức, doanh nghiệp phải làm việc từ xa theo chính sách, quy định của nhà nước tuy nhiên chưa đảm bảo an toàn thông tin dẫn đến bị lộ lọt, chiếm đoạt. Theo thống kê của Viettel Threat Intelligence, số lượng lỗ hổng được phát hiện và công bố trong quý 1 năm 2022 tăng 33,31% so với cùng kỳ năm 2021. Số liệu Cloudrity thống kê quý II/2022:

16,933,145
Tấn công khai thác lỗ hổng web

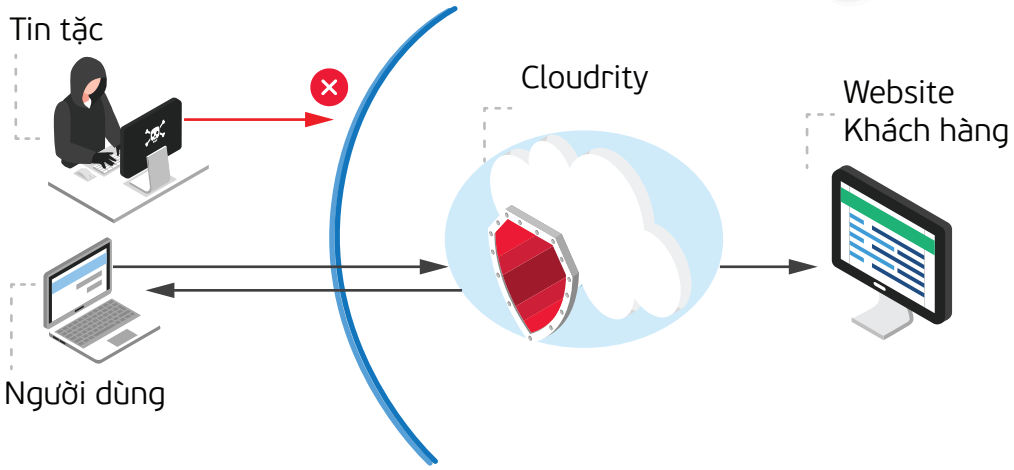
9,152,589
Tấn công DDoS L4

152,328
Tấn công DDoS L7



Dịch vụ bảo vệ website Cloudrity ra đời nhằm bảo vệ tốt nhất cho website khách hàng trước các cuộc tấn công có chủ đích từ bên ngoài, qua đó bảo vệ hoạt động sản xuất kinh doanh của khách hàng.

Mô hình hoạt động



Datasheet
VIETTEL CLOUDRITY

Các gói dịch vụ của Cloudrity

Tính năng	Mô tả	Gói dịch vụ		
		WP Silver	WP Gold	WP Platinum
Tường lửa ứng dụng web	Chống tấn công thuộc Top 10 OWASP - top 10 lỗ hổng bảo mật web phổ biến nhất theo tiêu chuẩn OWASP. Những lỗ hổng này cho phép tin tặc khai thác, tấn công và xâm nhập dữ liệu của website.	Cơ bản*	Đầy đủ*	Đầy đủ*
	Ngăn chặn khai thác lỗ hổng 1-day, những lỗ hổng đã được công bố của web frame-work, web server, mail server, ... Những website sử dụng phiên bản cũ chưa được vá các lỗ hổng của các công nghệ này có nguy cơ bị tin tặc khai thác.		✓	✓
	Bổ sung luật tùy chỉnh chặn theo nhu cầu	✓	✓	✓
Chống tấn công DDoS	Chống tấn công DDoS tầng mạng (DDoS L4) - các dạng tấn công volume lớn như UDP Flood, SYN Flood.	1Gbps	5Gbps	Theo yêu cầu
	Chống tấn công DDoS tầng ứng dụng (DDoS L7) - các dạng tấn công như HTTP Flood, Slow loris	500Mbps	2Gbps	Theo yêu cầu
	Ngăn chặn bot với cookie challenge	✓	✓	✓
	Tần suất truy cập tối đa	1000rps	5000rps	Theo yêu cầu
	Giới hạn tần suất truy cập từ mỗi IP nguồn (theo số lượng request, số lượng connection)	✓	✓	✓
Danh sách truy cập	Quản lý danh sách IP blacklist/whitelist	✓	✓	✓
	Quản lý danh sách URI whitelist	✓	✓	✓
Giám sát	Giám sát băng thông truy cập (bps, rps, cps, pps)	✓	✓	✓
	Giám sát sự kiện tấn công (WAF, DDoS L7)	✓	✓	✓
Báo cáo	Báo cáo định kỳ gửi tự động	✓	✓	✓
	Báo cáo tùy chỉnh			✓
Cảnh báo	Cảnh báo downtime website qua SMS			✓
Các tính năng khác	Hỗ trợ IPv6	✓	✓	✓
	Hỗ trợ CNAME	✓	✓	✓
Cam kết chất lượng dịch vụ	Cam kết uptime (cả khi xảy ra tấn công)		99.99%	99.99%
	Hỗ trợ 24/7		✓	✓
	Hotline hỗ trợ khẩn cấp		✓	✓
	Thời gian phản hồi yêu cầu xử lý Cấp độ 1*		Tối đa 2 giờ	Tối đa 30 phút
	Thời gian phản hồi yêu cầu xử lý Cấp độ 2*		Tối đa 4 giờ	Tối đa 1 giờ
	Thời gian phản hồi yêu cầu xử lý Cấp độ 3*		Tối đa 24 giờ	Tối đa 8 giờ

Ghi chú

Cơ bản*: gồm các rule cơ bản nhất, có thể bật tường lửa ứng dụng web ngay, tỷ lệ lỗi chặn nhầm (False-Positive) thấp.

Đầy đủ*: gồm đầy đủ tập rule OWASP, chặt chẽ hơn, nhưng tỷ lệ lỗi chặn nhầm cao hơn, phải tối ưu tập rule trước khi bật tường lửa ứng dụng

Cấp độ 1*: những sự cố nghiêm trọng ảnh hưởng đến độ khả dụng (Uptime) của toàn bộ dịch vụ.

Cấp độ 2*: những lỗi ít nghiêm trọng, hoặc lỗi chặn nhầm.

Cấp độ 3*: yêu cầu cập nhật cấu hình, hỏi đáp.