CDNetworks

Tường lửa ứng dụng web (WAF)

Bảo vệ thông minh các ứng dụng web trong thời gian thực

Tường lửa ứng dụng web (WAF) của CDNetworks là một giải pháp dựa trên đám mây giúp bảo vệ các ứng dụng web khỏi các cuộc tấn công web độc hại, vá các lỗ hổng bảo mật trước khi chúng có thể bị khai thác, loại bỏ các điểm yếu, bảo vệ chống lại các loại tấn công khác nhau và giảm thiểu rủi ro. Sử dụng nền tảng phân tích dữ liệu lớn để thu thập dữ liệu và mẫu tấn công hàng ngày, giải pháp WAF của chúng tôi phân tích các dữ liệu này để tối ưu hóa các quy tắc WAF, cung cấp bảo vệ chống lại các lỗ hổng trong danh sách OWASP Top 10.

Dịch vụ phân tích thông minh

Dịch vụ phân tích thông minh của WAF sử dụng trí tuệ nhân tạo (AI) và thuật toán học máy (ML) để nhận diện các yêu cầu hợp lệ của người dùng bị chặn nhầm bởi các quy tắc WAF, đồng thời tạo ra các ngoại lệ cho các quy tắc đó, giúp giảm thiểu cảnh báo sai.

Bảo vệ Zero Day

Luôn theo dõi các lỗ hổng Zero Day mới, giải pháp WAF của CDNetworks sẽ ngay lập tức gửi "bản vá ảo" thông qua các quy tắc WAF đến toàn bộ nền tảng và nhanh chóng xử lý khi phát hiện các lỗ hổng Zero Day.

Nhiều công cụ trực quan hóa

Giải pháp WAF của CDNetworks cung cấp nhiều công cụ trực quan hóa khác nhau như bảng điều khiển WAF, nhật ký sự cố, đồng bộ hóa nhật ký với hệ thống SIEM và cảnh báo tấn công, giúp bạn luôn cập nhật tình trạng bảo mật của tổ chức và điều chỉnh các quy tắc WAF để tăng cường bảo vệ cho doanh nghiệp.

Liên hệ qua **sales@cdnetworks.com** hoặc truy cập **cdnetworks.com**

Tính năng

Phòng thủ theo OWASP Top 10

Hơn 1.000 rules WAF tích hợp sẵn được cung cấp để bảo vệ khỏi các mối đe dọa hàng đầu được OWASP công bố, như tấn công injection, path traversal, XSS và nhiều hình thức khác.

Rules tùy chỉnh

Tăng tính linh hoạt trong bảo vệ bằng cách tạo các quy tắc tùy chỉnh và mẫu nhận diện thông qua trình hướng dẫn quy tắc thân thiện với người dùng.

Xác thực giao thức HTTP

Cung cấp nhiều tiêu chí cài sẵn cho việc xác thực giao thức HTTP, cho phép tổ chức cấu hình, phát hiện và chặn các yêu cầu HTTP bất hợp pháp dựa trên các yếu tố như phương thức yêu cầu, phiên bản và kích thước header.

Kiểm soát truy cập

Chặn người dùng bất hợp pháp và lưu lượng truy cập độc hại tiềm ẩn dựa trên địa chỉ IP, header HTTP và các thuộc tính khác nhằm ngăn chặn các cuộc tấn công vào ứng dụng web.

Giới hạn tốc độ truy cập

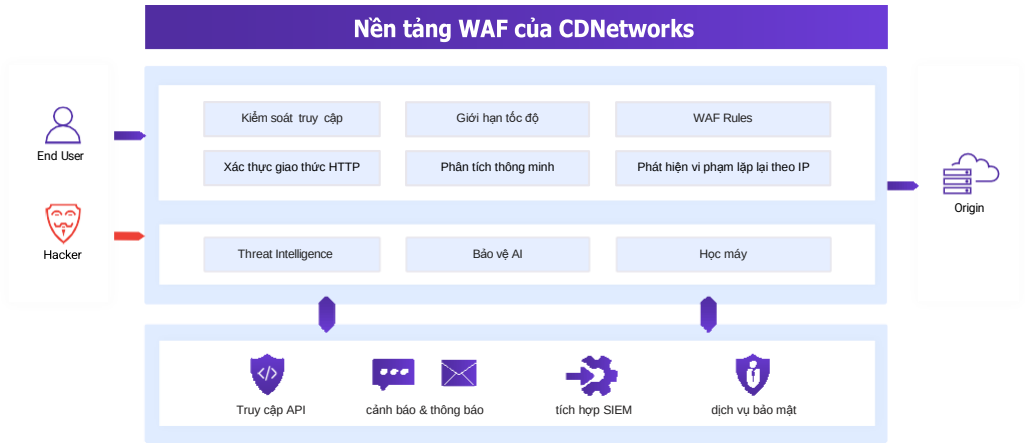
Giảm nguy cơ tấn công brute-force và các hình thức tấn công tự động khác bằng cách cấu hình số lượng yêu cầu HTTP được phép gửi đến máy chủ backend trong một khoảng thời gian nhất định.

Threat Intelligence

Cung cấp cho tổ chức lượng lớn dữ liệu IP từ bên thứ ba để chủ động đưa vào danh sách đen các địa chỉ IP có khả năng gây hại trước khi xảy ra tấn công.

Cách hoạt động

WAF của CDNetworks là một giải pháp dựa trên nền tảng đám mây, tích hợp hơn 1.000 rules WAF có sẵn. Với các rules này, cùng với các quy tắc tùy chỉnh, kiểm soát truy cập, giới hạn tốc độ truy cập, threat intelligence và các tính năng khác, giải pháp WAF của CDNetworks có thể giám sát và chặn các yêu cầu độc hại từ các cuộc tấn công web theo thời gian thực.



Ứng dụng công nghệ trí tuệ nhân tạo (AI) và học máy (ML), giải pháp này tự động xử lý các sự cố tấn công ở chế độ ngoại tuyến và tạo ra các chiến lược phòng thủ mới nhằm tăng cường bảo vệ cho doanh nghiệp của bạn.

Ngoài ra, WAF dựa trên nền tảng đám mây của chúng tôi được triển khai tại các nút biên trên toàn cầu, cho phép chặn các yêu cầu tấn công gần nguồn phát tán, qua đó tăng cường khả năng bảo vệ cho toàn bộ hệ thống phòng thủ.

Theo dõi tại

Bắt đầu dùng thử miễn phí

Liên hệ qua **sales@cdnetworks.com** hoặc truy cập **cdnetworks.com**