

Ngăn chặn các cuộc tấn công DDoS bằng A10 Defend:

Giải pháp ngăn chặn các cuộc tấn công DDoS toàn diện cho doanh nghiệp



DDoS vẫn là mối đe dọa lớn nhất. Các phương án phòng thủ nhiều lớp và đa vector là những biện pháp rất cần thiết. Giải pháp ngăn chặn các cuộc tấn công DDoS của A10 là một giải pháp trọn gói giúp phát hiện, giảm thiểu, điều phối và cung cấp thông tin chuyên sâu về DDoS, mang đến lớp phòng thủ chính xác, thông minh, chủ động và có thể mở rộng để đương đầu trước các cuộc tấn công tinh vi hiện nay. Sở hữu thiết kế tích hợp liền mạch, Giải pháp bảo vệ của A10 đảm bảo mang đến hàng rào bảo vệ cao nhất, đồng thời duy trì hiệu quả hoạt động, bảo vệ cơ sở hạ tầng trước mối đe dọa DDoS ngày càng lớn.



Ngăn chặn
mối đe dọa

Ứng dụng 1: Ngăn chặn mối đe dọa

Giải pháp ngăn chặn mối đe dọa dựa trên đám mây của A10 dưới dạng SaaS giúp bảo vệ doanh nghiệp của bạn với rất ít sự gián đoạn. Không đòi hỏi bạn phải trang bị những thiết bị DDoS chuyên dụng, giải pháp này củng cố hàng rào ngăn chặn DDoS với dữ liệu và phân tích chuyên sâu mà không suy giảm.

Nền tảng thông tin chuyên sâu về DDoS của A10 cũng có thể tạo ra các danh sách chặn thông minh để chủ động ngăn chặn các mối đe dọa trước khi chúng gây ảnh hưởng đến hoạt động của bạn. Bạn có thể dễ dàng tích hợp các danh sách này vào cơ sở hạ tầng an ninh hiện có của mình để sở hữu một hệ thống bảo vệ thống nhất và hiệu quả trước những mối đe dọa ngày càng tinh vi và tăng mạnh.



Phát hiện
mối đe dọa

Ứng dụng 2: Phát hiện mối đe dọa

Giải pháp phát hiện mối đe dọa DDoS của A10 mang lại khả năng phát hiện nhanh chóng, chính xác bằng phương pháp dựa trên luồng, nhận diện các mối đe dọa tiềm ẩn chỉ trong vòng ba giây. Khả năng phát hiện nhanh chóng này giúp khách hàng giảm thiểu thời gian ngừng hoạt động và duy trì khả năng

cung cấp dịch vụ ngay cả khi bị tấn công. Sự linh hoạt của giải pháp này càng củng cố thêm khả năng phát hiện mối đe dọa DDoS mà không làm gián đoạn hoạt động hiện tại.



Giảm thiểu
mối đe dọa

Ứng dụng 3: Giảm thiểu mối đe dọa

Giải pháp giảm thiểu mối đe dọa DDoS của A10 mang đến khả năng bảo vệ mạnh mẽ, theo thời gian thực trước cả các cuộc tấn công DDoS theo khối lượng và theo lớp ứng dụng, đảm bảo doanh nghiệp của bạn vẫn duy trì hoạt động trực tuyến ngay cả khi phải đối mặt với những mối đe dọa nghiêm trọng nhất.

Với khả năng tự động báo cáo sự cố, A10 có thể ngăn chặn thiệt hại một cách thông minh mà không cần sự can thiệp của con người. Giải pháp này có thể triển khai trực tiếp hoặc tích hợp qua định tuyến BGP hoặc DNS. Đối với các doanh nghiệp có lưu lượng truy cập tăng đột biến, A10 hiện cung cấp giải pháp lại giảm thiểu DDoS qua đám mây, chuyển hướng lưu lượng truy cập khi cần thiết để liên tục đảm bảo an ninh và duy trì thời gian hoạt động.

Lợi thế của giải pháp ngăn chặn các cuộc tấn công DDoS bằng A10 Defend

- ✓ **Đón đầu các mối đe dọa:** Tận dụng thông tin chuyên sâu, chính xác mà không suy giảm để phát hiện và chặn đứng các cuộc tấn công trước khi chúng làm gián đoạn hoạt động kinh doanh của bạn.
- ✓ **Duy trì hoạt động liên tục:** Khả năng giảm thiểu tấn công tự động, thông minh và linh hoạt giúp đảm bảo doanh nghiệp của bạn duy trì hoạt động, ngay cả trong các cuộc tấn công quy mô lớn.
- ✓ **Quy trình bảo vệ đơn giản:** Khả năng điều phối chuyên dụng giúp giảm bớt sự phức tạp và thời gian phản hồi, cũng như tăng độ chính xác để khôi phục nhanh hơn.

Các cuộc tấn công từ chối dịch vụ vẫn rất phổ biến và là kiểu sự cố thường gặp nhất.

— Báo cáo Điều tra Rò rỉ Dữ liệu của Verizon 2024

Nguồn: [verizon.com/business/resources/Tfd3/reports/2024-dbir-data-breach-investigations-report.pdf](https://www.verizon.com/business/resources/Tfd3/reports/2024-dbir-data-breach-investigations-report.pdf)

Hãy liên hệ với chúng tôi để lên kế hoạch cho giải pháp của bạn

apac@a10networks.com
A10Networks.com

