DDoS Defense Amplification Platform:

Comprehensive DDoS Defense: Visibility, Protection, Reports/Advisories

Amplify or Establish DDoS Defense With a Comprehensive and Proactive Approach

DDoS, the number-one threat incident, drives the need for specialized defenses. Existing DDoS protection that just relies on hardware or cloud scrubbing can stop basic DDoS attacks. Basic is not enough. Due to the complexity and volume of modern-day DDoS attacks, supplementary DDoS defense that is more accurate and proactive is needed. With the complexity of infrastructures, it is important that supplementary DDoS defense be easy to integrate and deploy. **A10 Defend Threat Control, a comprehensive DDoS defense platform, enhances DDoS visibility, provides DDoS protection, and enables proactive DDoS threat investigation.**

Use-case 1:

A10's proprietary AI-enhanced methodology of collecting and validating data allows Defend Threat Control to provide both proactive and defensive insights that are exceptionally accurate. Organizations deploying Threat Control can gain an adversarial perspective of their network or conduct in-depth research on external threats worldwide. DDoS attacks can be conducted irrespective of the vector used and can be just as easily executed using lesser-known attack vectors, as indicated by the recent http2 rapid reset vulnerability. These insights provide recommendations for adjusting organizational infrastructures and ensures visibility on many more potential DDoS attack vectors.

AI-enhanced Granular Insights

Use-case 2:

A10 Defend Threat Control's actionable block lists use A10's proprietary discovery and validation methodology. This ensures the lists are highly accurate, actionable, and easily digested by existing security devices. The result is a first layer of DDoS defense for organizations currently missing a DDoS prevention system. If the organization has existing DDoS prevention, Threat Control's block lists can easily be added to more comprehensively investigate and protect against DDoS, amplifying the effectiveness of the existing DDoS prevention system. These block lists adhere to organization-specific customizations and ISP guidelines. Consequently, this ensures that the lists are more effective and tailored to the specific needs of an organization. Additionally, it enables the deployment of these lists to the organization's ISP, serving as an additional layer of defense during an active DDoS attack.

High-confidence, Actionable Block Lists

The A10 Defend Threat Control Advantage

- Supplement existing DDoS defense, or establish accurate first layer of defense without requiring DDoS hardware
- Gain valuable insights, stop DDoS attacks, and inject proactive DDoS defense
- Monitor and investigate potential threats and gain adversarial perspective of your network

> *Denial of Service attacks continue to be ubiquitous and have remained in the top spot of incidents for several years now.*
>
> — Verizon 2023 Data Breach Investigations Report

Source: verizon.com/business/resources/Tbc9/reports/2023-data-breach-investigations-report-dbir.pdf

Contact Us for a Solution Planning Session

1-888-A10-6363
A10networks.com