DATA SHEET

A10 Defend Threat Control

A Necessary and Proactive DDoS Attack Intelligence

A10 Defend Threat Control, a component of the A10 Defend suite, is a necessary supplement required to combat the increasingly complex and rising number of DDoS threats. Establishing a DDoS attack intelligence presence, A10 Defend Threat Control provides a proactive and detailed list of DDoS weapons and can deliver actionable insights to help organizations thwart attacks by blocking malicious IPs that can launch or amplify DDoS attacks.

DDoS: Escalating Threat Landscape

Don't underestimate DDoS attacks. They may not be on the hype cycle, or nearly talked about enough, but they are continuing unabated. Now, in part because of the growth of IoT devices, the exponential rise in the importance of maintaining system uptime, availability, and brand reputation, DDoS is becoming an increasingly dangerous threat. It is critical to stay ahead of and understand potential attacks to safeguard your organization's reputation and ensure uninterrupted system availability.

DDoS attacks have evolved for numerous reasons, such as the adoption of innovative methods like carpet bombing. Additionally, the exponential growth of global internet connectivity has resulted in an expanded network of online devices. This then multiplies the number of origin points for DDoS attacks.

To comprehensively thwart these evolved DDoS threats, proper implementation of AI/ML, scalability, automation, and advanced techniques outside of just rate-limiting are needed. However, two additional capabilities of DDoS defense are required. First, a layered defense is needed to help lessen the strain on security teams, optimize cloud scrubbing usage, counter the complexity and volume of DDoS attacks, and lower TCO. Second, security teams need actionable insights that account for the nuances of each protected infrastructure. This way, an administrator can adjust configurations based on trends and analytical insights. A10 Defend is a holistic DDoS defense suite that provides in-depth, layered defense and includes the actionable insights of A10 Defend Threat Control.

SaaS

A10 Defend Threat Control

Related Products & Services

A10 Defend Mitigator

A10 Defend Detector

A10 Defend Orchestrator

DSIRT Support

Talk with A10

A10Networks.com/a10-defend

Proactive DDoS Insights and Defense

A10 delivers intelligence that focuses specifically on DDoS threats. It has built a DDoS attack intelligence platform that combines proprietary data gathering, validation and analysis, curated into actionable defense tools. Intelligence is not a panacea, but with the increasing volume and complexity of DDoS attacks, it is a necessary supplement.

Security teams can use A10 Defend Threat Control's customized blocklists to address the specific needs of an organization. Traditional intelligence is often crowd-sourced, stale, and broader in scope. A10 Defend Threat Control's DDoS-specific intelligence is vendor-agnostic, thoroughly researched, frequently updated, and much more in-depth.

This allows organizations to leverage A10 Defend Threat Control's customizable block lists to address their specific needs. These blocklists can be deployed alongside existing DDoS defense, or they can be used to bolster DDoS defense. A10 Defend Threat Control's custom blocklists can be ingested by most existing security devices.

Unlike other tools available today that provide convenience at the cost of false positives and false negatives, A10 Defend Threat Control's hands-on insights into attackers, victims, analytics, vectors, trends, and other characteristics can help establish a more robust and comprehensive security posture, tailored for thwarting DDoS attacks.

Key Benefits

Lower

Your TCO

In hybrid or cloud DDoS solutions, reduce the number of swings to the cloud, or conserve cloud scrubbing capacity by deploying accurate, customized blocklists. Establish a reliable first layer of DDoS defense without the need for dedicated hardware or more expensive cloud scrubbing services. Administrators with a thorough understanding of existing infrastructure can leverage valuable insights.

Thwart

Emerging Threats

A10 Defend Threat Control employs a proprietary data gathering and validation method to provide accurate, actionable, and intelligent data that can greatly bolster a DDoS defense. Insights into trends, vectors, and how the attackers are attacking and how the victims are responding can help an organization develop a more comprehensive DDoS defense scheme that can be prepared against known and unknown DDoS threats.

Augment

Your DDoS Defense

A10 Defend Threat Control can operate as a standalone SaaS platform, establishing DDoS defense without dedicated hardware or its block lists can be ingested and used with existing security devices such as routers or firewalls. zCustomized and automated block lists act as a first layer of defense and are particularly effective in managing the volume and complexity of modern multi-vector DDoS attacks, which are characterized by record-setting intensity and new and complex attack vectors.

Examining the DDoS Threat Landscape

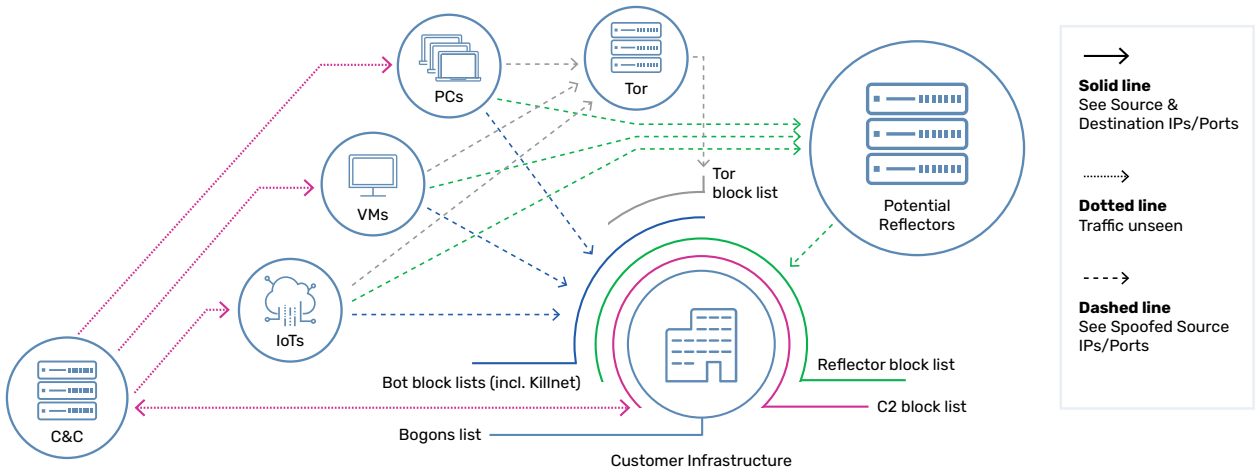

Figure 1: The expanding threat landscape

A customer's infrastructure is vulnerable to DDoS threats from multiple sources. Malware could be running on PCs, virtual machines, or other IoT devices. Command and Control servers, which are the central hub for attackers to manage and orchestrate their attacks, are the true source of attacks. Legitimate "open" servers on the internet can be compromised through a variety of attack vectors to launch reflection attacks. Proxy servers, such as Tor, can redirect attacks, masking the origin source.

The zero-atrophy characteristic of the three custom, proprietary blocklists that A10 provides is the main differentiator.

- C2 list: A10's advanced analysis can determine C2 servers by reverse-engineering malware within contaminated systems that have been recruiting other systems for botnets. This compact, DDoS-focused list provides high-confidence, and can block the origin source of an attack. This capability is critical in taking down entire botnets. Attempting to stop individual bots without being able to target the root cause is like playing a losing game of whack-a-mole.
- Bot list: A10's proprietary data gathering and validation method analyzes the behaviors and characteristics of attacks launched by malware-compromised systems. Through continued analysis of vast accumulated data, A10 Defend Threat Control can confidently generate a list that identifies which entities may be participants of botnets.
- Reflector list: Reflectors are systems configured to amplify responses, generating significantly larger responses than the original requests. These systems play a crucial role in amplification attacks, where the objective is not to flood the target with numerous requests, but to overwhelm it with a small number of requests that trigger disproportionately large responses. Identifying potential reflectors is helpful. While they may not currently pose a threat, their configuration and status leaves them vulnerable to potential exploitation.

Features

Multi-dimensional

Dashboard

The real-time DDoS attack map and accompanying details help to visualize the state of DDoS attack incidents around the world, both from an attack and victim perspective. Attack trends over time are presented using logarithmic and linear charts. Advanced filtering is also available and able to drill down by attack vector parameters such as geolocation, duration, historical data, protocol, port, and others. These insights and findings can be downloaded in pdf reports for further analysis.

Meticulous

Victim Identification

DDoS attacks are not solely executed through the top-two or three attack vectors. New, undiscovered vectors and methods of attack are constantly being explored. A10 Defend Threat Control's actionable insights provide unprecedented visibility into reflectors, botnets, and indicators of compromise. These insights are further classified by country, organization, and other characteristics. Additional insights include visibility into victim IP ranges, victim ASNs, top malware hashes, ports scanned, protocols exploited, total number of DDoS weapons by classification, and others. These insights, in the form of attack research/IP search, along with alerts and notifications for included IPs, empower administrators to properly configure and prepare their infrastructures, safeguarding against the latest and more severe DDoS threats.

Flexibility

and Convenience

As a SaaS platform, A10 Defend Threat Control has convenient capabilities such as single sign-on, multitenancy, notification management, open search, and more. The user-friendly audit trail is intuitive, enabling simplified management of users, tenants, and sessions.

Data

Perpetuation

A10's proprietary data gathering and validation method generates zero-atrophy data, which never gets stale and is always up to date. This is important because attack vectors are constantly evolving, and at-risk configurations vary constantly. Without real-time information and fresh updates, it can become ineffective.

Dualistic

Baselining and Profiling

A10 Defend Threat Control presents an attackers' view of your infrastructure, and helps users understand which vulnerabilities can potentially be exploited by attackers. When searching by IP address/network, users can see if an IP address/network is "under attack," or if it is being "weaponized." Reports and advisories can be used in tandem with these insights for granular analysis.

Impactful

IP Blocklists

A10 Defend Threat Control provides ease of operation, enabling users to deploy a new DDoS defense, or bolster the existing DDoS defense, quickly and easily. High-confidence and customizable DDoS-specific block lists can be generated for botnets, reflectors, and command & control. Open-source block lists are also available for the Killnet botnet, Tor proxy, and IP bogons. Blocklists can easily be ingested by any existing security device, or the SIEM device in place. Special use-cases can be supported. If the user is looking to integrate the whole dataset, Defend Mitigator has the capacity to ingest 96 million blocklist entries.

Learn More

About A10 Networks

Contact Us

A10networks.com/contact

Part Number: A10-DS-15139-EN-01 Mar 2024