eBOOK

SUPERCHARGE YOUR DDoS PROTECTION STRATEGY

Precision, Scalability, Automation and Affordability:
four principles of an impermeable DDoS defense solution

INTRODUCTION

DDoS attacks plague organizations of all sizes and across all industries. The frequency, intensity and sophistication of modern attacks—and attackers—threaten the most crucial aspect of running an online business with 24/7 availability.

The high costs of downtime are well documented, as are the devastating effects of DDoS attacks. The proliferation of Internet of Things (IoT) devices exacerbates these problems. Shrewd attackers have harnessed unsecured devices and turned them into massive botnets that are capable of launching paralyzing DDoS attacks that can exceed 1 Tbps. (For information about the IoT DDoS invasion, read our infographic.)

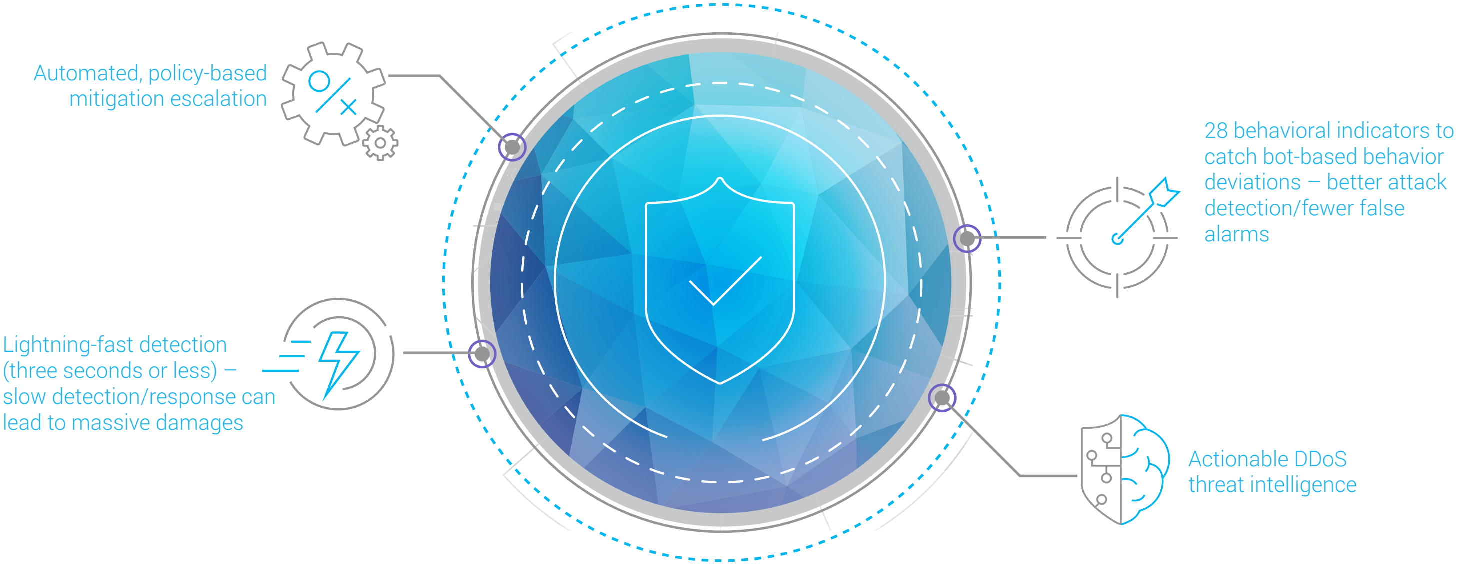
This eBook is designed to help you understand the four critical principles behind an impermeable DDoS defense so that you may evaluate and choose the best DDoS solution for your organization.

1

Legitimate Users Matter — Defend Them with Surgical Precision

Many of the commonly used legacy DDoS solutions that are currently available were developed back in the 2000s when protecting network infrastructure from attacks was paramount. Times have changed, however, and legitimate users need to be more than a mere afterthought.

Maintaining service availability during a DDoS attack is the primary reason to deploy a DDoS protection solution. Even if your system withstands the attack, if the legitimate users can't access the tools they need, your solution has failed. Effective DDoS defenses need to be precise, with the ability to intelligently distinguish between legitimate traffic and attacking bots. Such a solution understands your environment—in peacetime and in wartime—and eliminates false reports. It leverages up-to-the-second traffic indicators and threat intelligence to pinpoint and eradicate bad actors.


Automated, policy-based mitigation escalation
28 behavioral indicators to catch bot-based behavior deviations – better attack detection/fewer false alarms
Lightning-fast detection (three seconds or less) – slow detection/response can lead to massive damages
Actionable DDoS threat intelligence

2

You Need Scale to Combat Modern DDoS Threats

Attacks continue to grow in size and sophistication. To be prepared, you need a solution that can defend against frequent and sophisticated attacks as small as 10 Gpbs, but robust enough to match those rare situations when they exceed 1 Tbps.

Attack size and breadth is another very important consideration when evaluating DDoS solutions. Attackers will expend as little effort as possible to cause the most damage. This can translate into millions of small packets from millions of bots against your network's firewalls and servers, instead of one massive volumetric flood.

Legacy defenses were built to defend against thousands of coordinating DDoS attack agents, not millions of weaponized IoT endpoints, meaning this persistent barrage of attack traffic can slip through. A hybrid DDoS defense solution ensures that you're capable of scaling. Combining an always-on, on-premise solution with a cloud scrubbing service for when your Internet pipe is overwhelmed ensures that your network can stand up to attacks at any scale.

To be prepared, you need a solution that can defend attacks as small as 10 Gpbs, but robust enough to match when they exceed 1 Tbps.

3

Automation Translates to Improved Efficiency

Have you ever tried to manage pure chaos? That's what DDoS attacks feel like from the inside. Legacy DDoS solutions require considerable manual intervention during wartime. According to a Neustar survey of organizations that suffered DDoS attacks, 45 percent were attacked six or more times, requiring an average of six people to defend against a single DDoS attack. Instead of working on tasks that benefit the business, people are pulled into a firefight.

Organizations need automated DDoS protection strategies that eliminate the manual intervention often required to defend against attacks. Leveraging automation based on pre-set policies maximizes effectiveness while minimizing the chances of false positives, thus preserving resources by keeping them focused on important tasks and not battling DDoS.

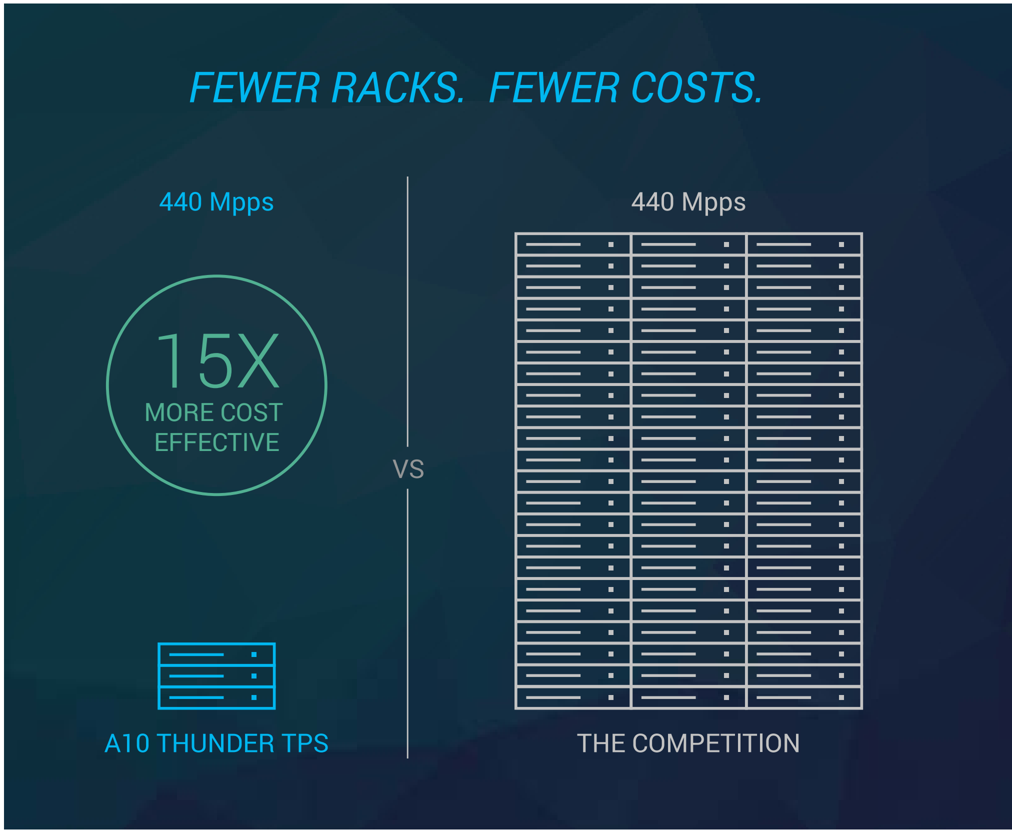
4

Affordability Counts

DDoS solutions tend to be quite costly, which is why switching between vendors can be a daunting proposition. However, moving away from a solution built on old technology in favor of a modern and more nimble solution can deliver a very high return.

To be affordable, solutions need to be high-performance, yet compact. One way to shrink spending on DDoS is to reduce your total footprint while still meeting or exceeding your organization's capacity requirements. This also trims hardware costs considerably, along with power, cooling, and data center rack space.

DDoS Defense for Today
Modern DDoS attacks require a new approach. Attacks are bigger, faster, wider, and more powerful than ever before. Legacy solutions can't keep up; therefore, they wither under the might of today's modern attacks. Rethinking DDoS isn't easy, but it does pay off in the end.



A10 THUNDER TPS

Thunder TPS® product line is a family of high-performance solutions that detect and mitigate multi-vector DDoS attacks at the network edge, functioning as a first line of defense for your network infrastructure.

The best-selling A10 Thunder 14045 mitigates DDoS attacks up to 300 Gbps with a single appliance and scales to 2.4 Tbps when deployed in a cluster.

▶ *LEARN ABOUT THUNDER TPS*

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide. For more information, visit: a10networks.com or tweet @A10Networks.

1-888-A10-6363 | a10networks.com

Part Number: A10-EB-14110-EN-01 MAR 2018