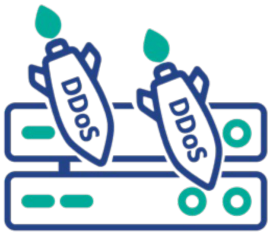
APPOSITE TECHNOLOGIES

DDoS Storm



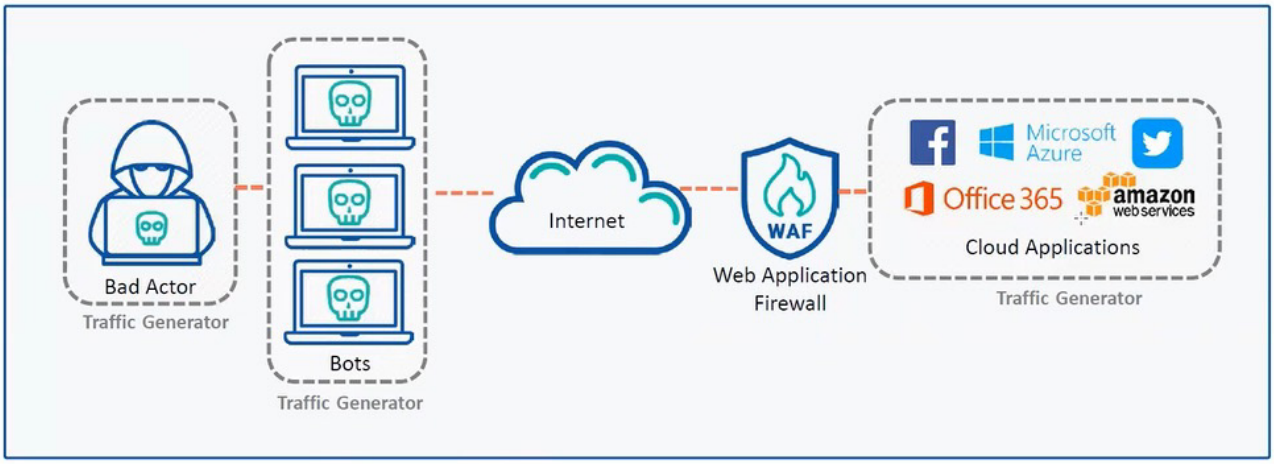
Traffic Generation Re-Imagined

Simulate Comprehensive DDoS Attacks at Tremendous Scale to Evaluate Defenses

OVERVIEW

Distributed denial of service (DDoS) threatens normal business operations as bad actors scale attacks. DDoS Storm simulates attacks that target layers 2-7 of your network simultaneously or unfold over time.

See how well — and quickly — DDoS protection, Web Application Firewalls (WAFs), and other tools identify and block malicious traffic without disrupting the flow of business. Validate DDoS protection before investing in new solutions and automate repeat testing to prevent new attacks as your threat landscape changes.



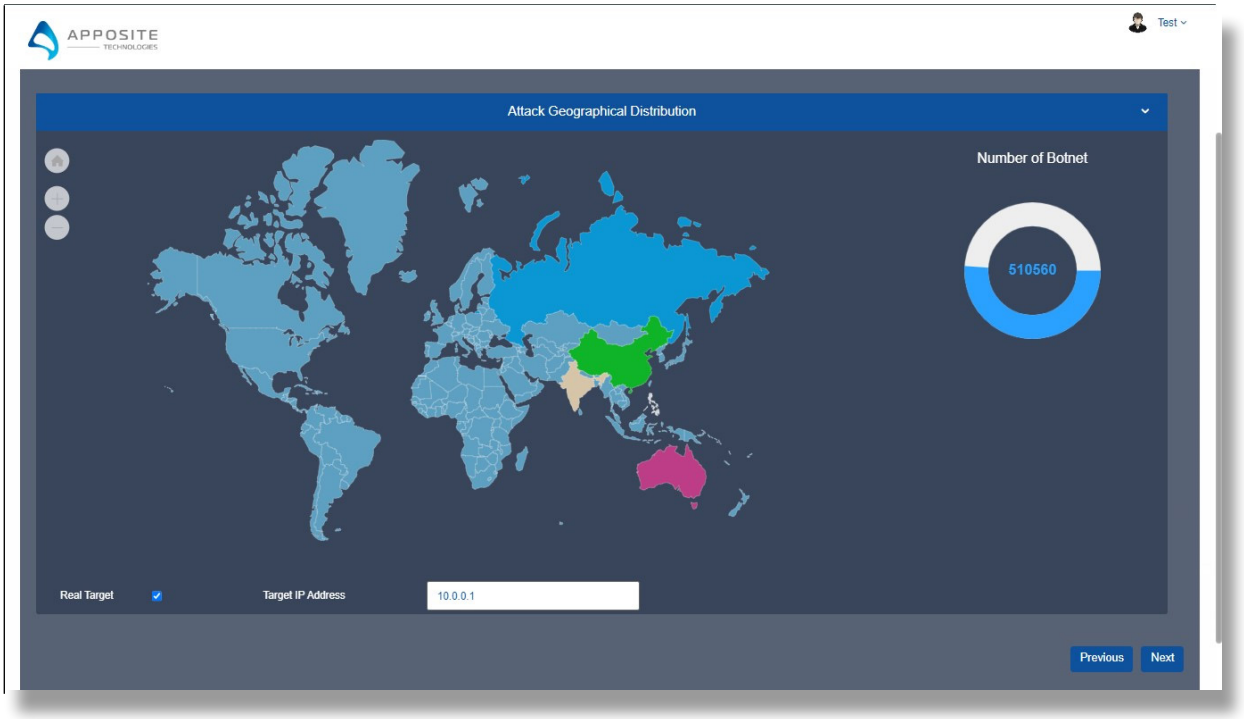
CAPABILITIES & BENEFITS

- Overwhelm network resources to test and optimize protection. Simulate DDoS attacks to evaluate the effectiveness of your prevention and mitigation strategies. See how well DDoS protection, Web Application Firewalls (WAFs) and other tools detect, block, and minimize the impact of attacks.
- Test your entire stack with one solution. Simulate multi-vector, multi-stage attacks against layers 2-7. Generate L2-3 attacks to test network-level vulnerabilities, switching, and routing to prevent network disruption and unauthorized access. Launch L4-7 campaigns targeting protocols and applications to protect data, user sessions, and app functionality.
- Find and fortify potential points of entry. Generate large volumes of legitimate and bot traffic from different regions simultaneously to identify potential entry points for attackers and fortify defenses accordingly.
- Protect uptime and service availability. Analyze the ability of devices under test (DUTs) to recognize and allow legitimate traffic amidst a flood of malicious requests.
- Test before you invest. Validate vendor performance claims and gauge the impact of new solutions on compliance and cyber insurance premiums.

FEATURES

- Test DDoS protection, alert, and mitigation against realistic attack scenarios at massive scale
- Simulate bad actors controlling hundreds of thousands of bots
- Generate attacks from L2 to L7 to evaluate every layer of the network stack
- Combine DDoS attacks with legitimate traffic
- Simulate attacks from specific regions and countries around the world
- Control how fast attacks ramp up and how often they repeat
- Combine and cycle attack vectors
- Act as the attacker (one port) or both the attacker and target (two ports)
- Validate defenses in closed-lab environments without disrupting operations

USER INTERFACE



Type of Attack	Layer Attacked	How it Works
Applicaitions (includes HTTP floods)	L7	Floods sites with HTTP requests, exhaust application resources consumes memory, CPU, etc
Protocol (SYN, ACK floods)	L3-L4	Destroys processing capabilities/exhausts resources of server/ network equipment resources (switches, firewalls, etc.)
Volumetric	L2	Sends large amounts of data to exhaust available bandwidth

DDoS Storm is available on high performance appliances and virtual machines. Configure tests with ease on the feature-rich, browser-based GUI or with our comprehensive RESTful API for increased automation. Run multiple tests at once and keep them running in the background, collaborate with your team, and easily connect and perform tests from anywhere.

Apposite Technologies

4223 Glencoe Ave, Suite B121, Marina Del Rey, CA 90292 USA

www.apposite-tech.com | TEL: 1.310.477.9955 | info@apposite-tech.com