DDOS Protection
Comprehensive Layer 3 to Layer 7 DDOS Coverage that Scales with Your Environment

The ThreatX platform provides a fully-integrated approach to the many risks and threats facing applications today. Defending organizations from the many forms of modern DDOS attacks is one of the key capabilities of this solution. Our approach protects organizations from application layer DDOS techniques as well as volumetric DDOS often seen at Layers 3 and 4. We provide offerings that align with the unique demands of any size organization, and our AppSec-as-a-Service (ASaaS) team of professionals is available "on-tap," 24/7 to help troubleshoot sophisticated attacks.

ThreatX DDOS Protection: Key Capabilities

» Automatically detect and prevent application layer DDOS using a combination of application profiling, bot detection, IP interrogation, and tarpitting.

» Automatically absorb all common DDOS attack techniques with on-demand burst capability for larger volumetric attacks

» SLAs tailored to fit your business needs and application environments

» Easily protect a single application or multi-application environments

» Always-on traffic monitoring and a 24/7 operations center for rapid and proactive response

» Real-time, executive level dashboards to monitor and analyze attacks as they happen

Application Layer DDOS Protection

Application layer or Layer 7 (L7) DDOS attacks can be some of the trickiest to mitigate and are often missed by traditional security tools. Attackers will use bots to mimic valid users and take advantage of an application's functionality. By taking advantage of faulty business logic or crafting highly intensive queries such as a database lookup, an attacker can overwhelm an application with a relatively small amount of normal-looking traffic. ThreatX uses multiple detection techniques and a combination of automated challenges, IP interrogation and tarpitting to ensure long-running queries, HTTP floods, and other L7 attacks are mitigated quickly and appropriately without impacting valid users.

Network Layer DDOS Protection

ThreatX provides highly scalable, low-cost protection from volumetric DDOS attacks which typically occur at Layers 3 and 4. With virtually no impact to end-users, the ThreatX standard DDOS coverage protects up to 100Gb of inbound traffic against sophisticated and large-scale attacks. The platform can scale on demand to even higher levels of traffic and is managed by ThreatX's 24x7 ASaaS to proactively identify appropriate response options and minimize impacts to customer systems.

Enterprise Class, Unlimited DDoS protection

ThreatX also provides additional DDOS attack protection services for customers with high bandwidth or service level requirements. ThreatX partners with multiple enterprise class L3/L4 DDoS providers with extremely large infrastructures capable of absorbing multiple-terabyte attacks. ThreatX actively manages these services through our 24x7 SOC, working with partners to identify and mitigate even the largest attacks in real time. Pricing varies and ThreatX will work closely with the customer to determine the optimal solution for requirements and budget available.

Technology Supported by Talent

DDOS attacks are often unpredictable and can strike at the most inopportune times. All ThreatX DDOS attack mitigation services are supported in real time by a dedicated team of highly trained AppSec experts. As situations and attack techniques morph, ThreatX will be there to help diagnose, respond and recommend.

Comprehensive Protection Against:

- » Bot behavior
- » Reflected ICMP & UDP
- » TCP SYN+ACK
- » TCP FIN
- » TCP RESET
- » TCP ACK
- » TCP ACK + PSH
- » TCP fragment

- » UDP
- » ICMP
- » IGMP
- » HTTP flood
- » Brute force
- » Connection flood
- » LRQ's
- » Spoofing

- » Mixed SYN + UDP or ICMP + UDP flood
- » Ping of death
- » Smurf
- » Teardrop
- » Zero-day DDOS attacks
  and more...

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

THREATX

SRC CYBER SOLUTIONS LLP