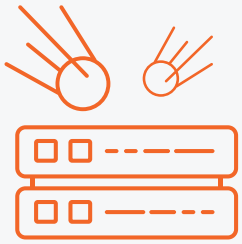
THREATX

DATA SHEET

DDoS Protection

Fully Integrated DDoS Protection That Scales

Savvy attackers know that they can map your applications to understand which pages or API calls consume resources such as memory, session handles, or CPU cycles. Armed with that information, they can design a sophisticated, multi-mode attack to consume resources, degrade your app's performance, and generally muddy the waters while trying more pointed exploits. *This is the outline of the modern distributed denial of service attack (DDoS).*



ThreatX provides attack protection against complex, multi-mode attacks including API abuse, distributed botnets, and DDoS attempts by delivering real-time protection on a scalable platform. ThreatX defends organizations from many forms of modern DDoS attacks and is one of the key pillars of an attacker-centric security solution.

Our attacker-centric behavioral-based detection protects organizations from today's increasingly prevalent Layer 7 (application-layer) DDoS attacks. ThreatX also has many customers that rely on our platform to scale and power protection against large-scale volumetric (Layer 3 and Layer 4) DDoS attacks.

Key Capabilities

- Sophisticated bot detection driven by behavioral analytics, active interrogation, and application analysis
- AI and ML single risk engine that detects and correlates threats across all API and web app assets by analyzing attacker behavior
- Real-time detection and blocking, deployed in-line as a reverse proxy to instantly stop attacks
- Automated blocking driven by risk-based scoring that ensures both extremely low false positives and low false negatives
- Managed services and security operations assistance, to ensure our customers get the highest protectiopossible from the ThreatX platform

Detect and Stop Bots

ThreatX uses a combination of entity analysis, active interrogation, and application analysis to distinguish bots from true human visitors. It starts by tracking an entity's behavior across many attempts, and if activity seems suspicious, ThreatX will engage with potential threats via active interrogation techniques like injecting fake fields or tarpitting traffic to see how the threat responds.

Other detection techniques allow for detailed fingerprinting and analysis of the host, and ongoing tracking allows the ThreatX platform to differentiate legitimate machine-to-machine communication from suspicious or malicious bot traffic.

Lastly, application analysis tracks how a threat is attempting to interact with an application. To detect and protect against large-scale botnet attacks — a powerful tool in DDoS attacks — ThreatX continuously analyzes the intensity of traffic to alert staff of any significant influxes of suspicious traffic.

Application-Layer DDoS Protection

Application or Layer 7 (L7) DDoS attacks can be some of the trickiest DDoS techniques to mitigate, and are often missed by legacy solutions. 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 of its resources with a relatively small amount of otherwise normal-looking traffic. ThreatX uses behavior-based detection and a combination of active interrogation techniques and tarpitting to ensure long-running queries, HTTP floods, and other Layer 7 attacks are mitigated quickly and appropriately without impacting valid users.

Network Layer DDoS Protection

ThreatX provides highly scalable protection against volumetric DDoS attacks on Layers 3 and 4. As part of our standard DDoS service, customers are protected against sophisticated, multi-mode attacks with our AI and ML behavior-based detection and real-time blocking that has no impact on inbound traffic. The solution can scale on demand to even higher levels of traffic by deploying our sensors on auto-scalers and co-deploying with L3/L4 solutions. ThreatX's 24x7 SOC proactively identifies appropriate response options and minimizes impacts to customer systems.

Enterprise-Class, Unlimited DDoS Protection

ThreatX also provides additional DDoS 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.

Technology Supported by Talent

DDoS attacks are often unpredictable and, by design, they strike at the most inopportune times. All ThreatX DDoS services are supported in real time by a dedicated team of highly trained application security experts. This means that even as situations and adversary techniques change, the ThreatX team is on the job to diagnose problems and respond in real time.

Comprehensive Protection

THREATX

The ThreatX platform provides comprehensive protection against a wide range of attack types. The platform detects and protects against:

Legacy, low-level DDoS attacks, such as:

- ✔ Reflected ICMP & UDP attacks
- ✔ ICMP and Ping floods
- ✔ UDP floods
- ✔ Mixed SYN + UPD or ICP + UDP floods
- ✔ Ping of Death
- ✔ ICMP Echo attacks, *aka Smurfing*

Layer 3 attacks:

- ✔ TCP SYN+ACK floods
- ✔ Bulk TCP resets
- ✔ TCP ACK floods
- ✔ TCL ACK + PSH attacks
- ✔ TCP fragment attacks

Layer -7 attacks:

- ✔ HTTP flood attacks
- ✔ Connection floods
- ✔ Zero-day exploits
- ✔ CVE exploits

Behavioral attacks, including:

- ✔ Suspicious or malicious bot traffic
- ✔ Brute force
- ✔ Spoofing
- ✔ Teardrop attacks

Attackers will often throw all these attack types together, into a sophisticated multi-mode attack, spanning tens of thousands of bots. You need protection that covers all the bases.

ThreatX's API and web application protection platform helps make the world safer by protecting APIs and web applications against complex, multi-mode attacks including DDoS attempts, credential stuffing, API abuse, account takeover, exploitations of zero-day vulnerabilities, and SQL Injection attempts. ThreatX effectively and efficiently protects APIs and web applications for companies in industries across the globe.