THREATX

TX Protect

Concepts

Version 3.20, 2025-01-10

The ThreatX platform gathers, organizes, and presents the data it collects into various pages and tables. The tables provide different perspectives of how the data relates to each other, which can help in your analysis.

Rules

A ThreatX WAF *rule* is a set of Boolean conditions that, when True, implement the rule's defined action and risk level. A True state is known as a match. The conditions are based on threat, request, or response attributes.

The rule's action is implemented by the ThreatX WAF sensor. The sensor also provides a curated set of common behavioral rules designed to identify risky behavior while minimizing false positives against legitimate users.

The ThreatX dashboard displays how often a rule is matched and implements its action. You can use this data to determine the effectiveness of each rule. As needed, you can request the ThreatX SOC group to create new rules or modify any rule in the ThreatX platform to meet the specific needs and behavior of your environment.

The ThreatX platform uses rules with advanced analyzers, IP interrogation techniques, and a combination of other detection capabilities working in parallel to observe traffic.

Sites

The ThreatX platform displays all the sites under the ThreatX protection, the API profile for each site, and every endpoint for each site.

Site	A *site*, also known as as an *API site*, is a web property serving API responses intended for consumption by an application.
Endpoint	An *endpoint* is a URL pattern representing a group of resources within a site. *(A site can have multiple endpoints.)*
Profile	The *API profile* refers to its type *(e.g., JSON, XML, or URL-encoded)*.

The ThreatX platform shows the sites by their **hostname**. You can drill-down to see a site's endpoints and the activity at each endpoint.

Threats

A *threat* is a representation of individual API clients or network of clients that have engaged in an activity that matches one or more rules and is therefore identified as suspicious or questionable. A threat is suspicious but not necessarily malicious.

Where it is common for attackers to use many IP addresses in a single attack, the ThreatX platform generates a name for each threat based on the IP addresses of the attacking entity. The name is in a human-readable format consisting of a "negative" adjective (such as Smelly) and a pirate name (such as Blackbeard) to identify each unique attacker.

The tables in the ThreatX dashboard offers analytical data about the threat. The following metrics are common to several tables.

Threat Metrics

Status	Current response to the threat. Status includes Watched, Blocked, Allow Listed, or Deny Listed.
IP Address	Origin of the threat.
Last Seen	Time of the last request.
Location	Country where the attack originated.
Attack Class	Category of the threat, such as XSS, password guessing, and Trojan activity.

Risk Score and Risk Level

There are two risk attributes:

Risk Score

This attribute is associated with a single activity of a threat, and is signature specific. The ThreatX platform displays Risk Score as a number between 0 and 100. The higher the score, the greater the risk.

Risk Level

This attribute is associated with all activities of a threat. The level is calculated from many inputs including Risk Score. One input is the kill chain model that classifies the attacker behavior and methods used to attempt to gain unauthorized access or control. The higher on the kill chain, the greater the severity of the threat. The ThreatX platform displays Risk Level severity as a bar. The longer the bar, the greater the risk.

Many of the tables in the ThreatX platform show **Max Level**, which is the maximum Risk Level in the specified time range.

Rule activity

Requests match a rule a certain number of times within a specific time range, which determines the Rule Activity. It is displayed as Intensity, either in exact numerical form or a simplified form (Low, Medium, High).

Matched rules are displayed in various tables. Clicking a rule name in the **Rules** column of a table displays that rule's activity page. Clicking a rule name in the **Description** column displays the properties for that rule.

Blocking Modes

There are three different blocking modes available for each site after on-boarding:

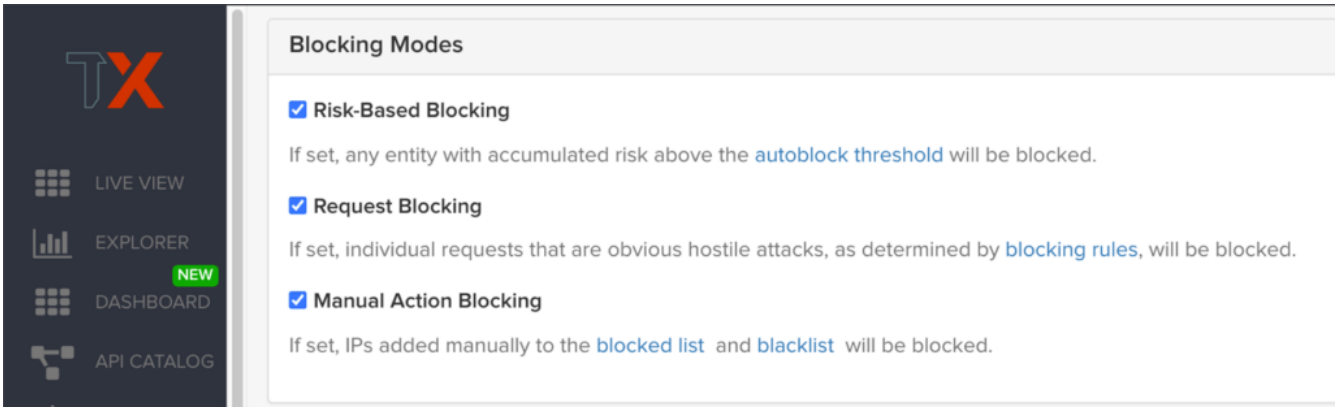

Figure 1. Blocking Modes

Request Blocking

When enabled for your sites, request blocking will block malicious traffic at the request level when an attack such as SQL injection, XSS, or another malicious request is detected.

Risk-Based Blocking

When enabled, risk-based blocking will allow ThreatX's behavioral analytics engine, hackerMind™, to evaluate each unique entity and block persistently malicious entities based on their behavior over time.

Manual Action Blocking

When enabled, this option permits manual blocking of specific IP addresses. Enabling also permits a ThreatX console user (security admin) to add entity IP addresses to the deny list for permanent blocking.

We recommend leveraging all three blocking modes, but provide users the flexibility to gradually expand blocking levels when on-boarding a new application to help prevent potential false positives or unwanted impacts to your sites.