



**THREATX**

TX Protect  
*ThreatX UI*

Version 3.20, 2025-01-10

# Table of Contents

Dashboard .....	3
API Catalog .....	15

# Introduction

After connecting hostnames to ThreatX, real-time attack information will be displayed via the Attack Dashboard and API Defender in the ThreatX platform. Use the latest available sensor version to see all information populated on the ThreatX platform.

The ThreatX platform provides metrics and analytical data of API traffic and actions taken to the dashboards and reporting pages. The ThreatX User Interface is off-site and hosted by the ThreatX SOC.

## UI Components

### Threat Response Platform

Sends metrics and analytical data and sends notifications using email or webhooks. You can respond manually using the allow, deny, and block lists.

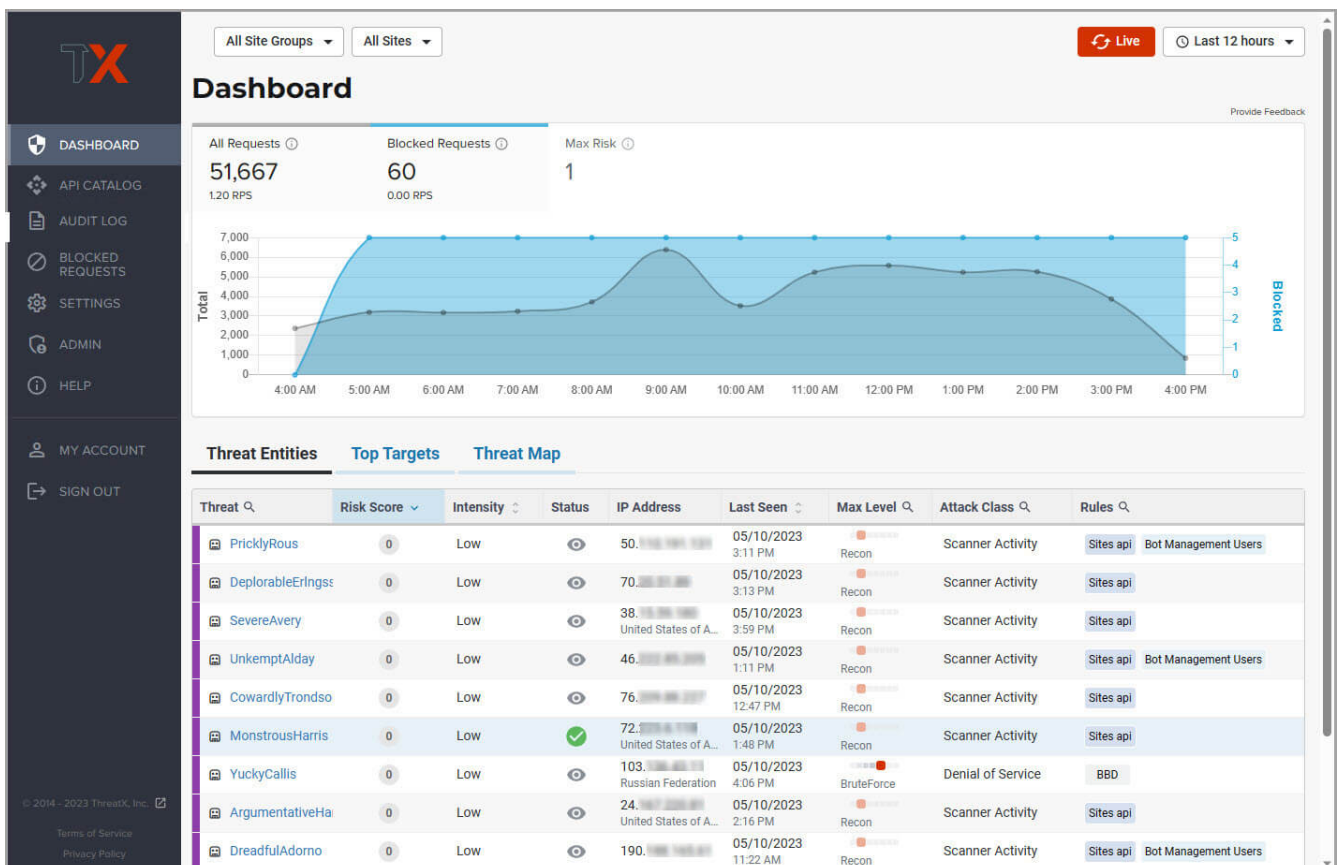
### Dashboard and Reporting

The ThreatX platform provides data in various forms including scorecards. You can drill down from a threat view to the individual endpoint. See the [Concepts](#) page for more information.

# Interfaces

The administrative settings can be accessed from the ThreatX user interface or API command line interface.

The ThreatX user interface presents the data the platform collects into various pages and tables. The ThreatX navigation bar has a **Settings** menu, under which you can access the pages discussed in this guide. You can log in to the ThreatX user interface at [x.threatx.io/](https://x.threatx.io/).



==

# Glossary

The ThreatX platform provides information about sites, endpoints, traffic, and threats and uses various terms to describe them. For clarity, the terms used in the ThreatX platform are defined as follows.

## API profile

Type of API such as JSON, XML, and URL-encoded.

## API traffic

Traffic that includes HTTP messages containing programmatic content sent between the site and client applications.

## Endpoint

URL pattern representing a group of resources within a site. A site can have multiple endpoints.

## Entity

A specific IP address or IP group. A suspicious entity is a *threat*.

## iWAF

Intelligent web application firewall. The next generation of the Web Application Firewall. See *WAF*.

## Non-API site

Site not served by an API server. Typically, a non-API site has web assets which are used for human interaction.

## Rule

Set of Boolean conditions that, when True, implement the rule's defined action and risk level. A True state is also known as a match.

## Sensor

See *WAF sensor*.

## Site

Web property serving API responses intended for consumption by an application. Also called an API site.

## Tenant

Container for an organizational unit such as a department or company. The ThreatX platform supports multiple tenants.

## Threat

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. An identified threat is not necessarily malicious.

## WAF

Web Application Firewall. Type of application firewall that applies specifically to web applications. It is deployed in front of web applications and analyzes bi-directional web-based (HTTP) traffic and detects and blocks anything malicious.

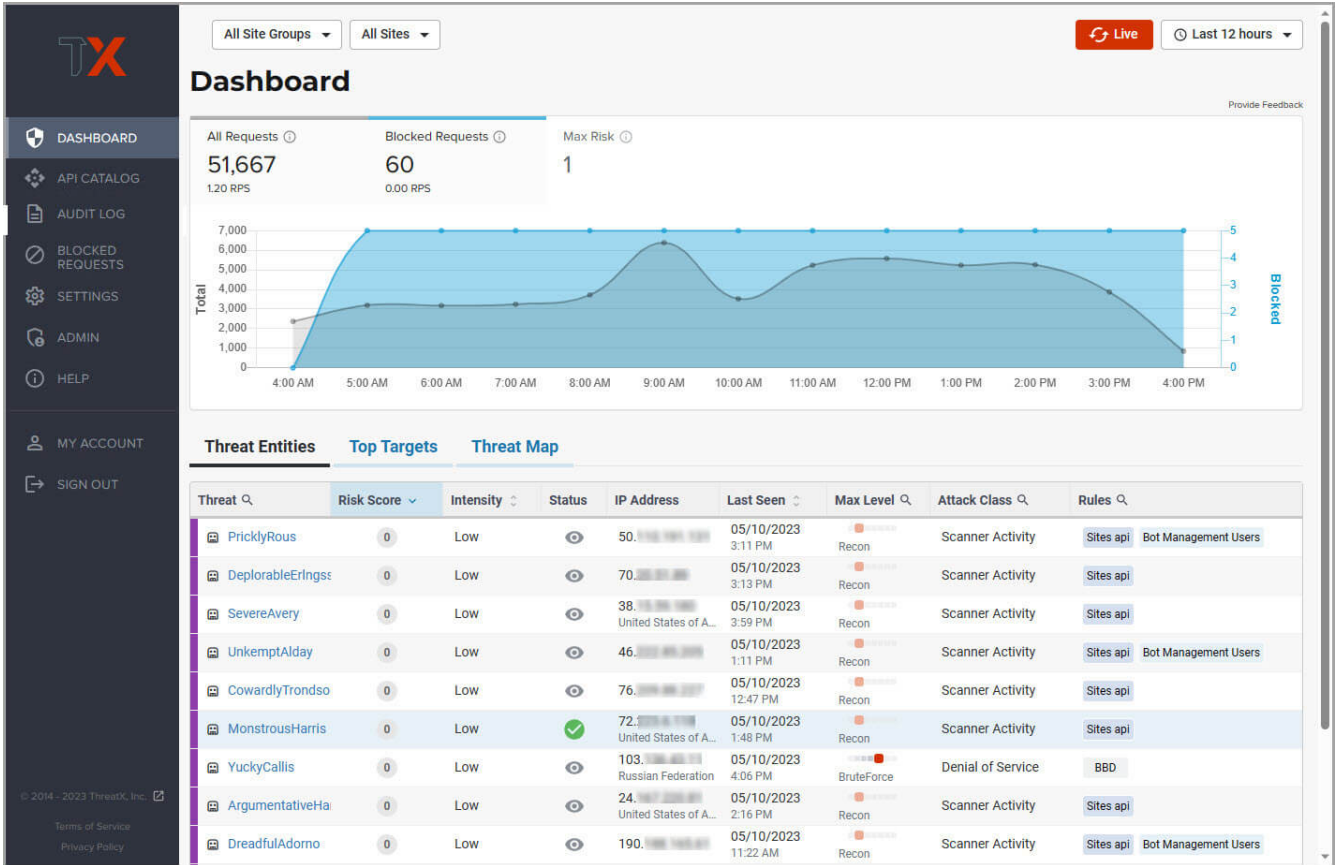
## WAF Sensor

A reverse proxy-based web application firewall. Sensors monitor all the HTTP(S) traffic flows for malicious and legitimate activity. The sensor is decoupled from the analytics platform, so it can be run anywhere in the world and is used by customers with high bandwidth requirements.

# Dashboard

## Introduction

The Dashboard, available from the navigation bar, displays essential data collected for each site in your environment under ThreatX protection. The data is live and driven by active site traffic.



## Attack Dashboard

### Threat Entities

The ThreatX Attack Dashboard visualizes both malicious and benign traffic over time and allows ThreatX users to drill down and investigate attacking entities, and the responsive actions the ThreatX Platform took to protect their APIs and web applications. The Attack Dashboard is comprised of three main views: Threat Entities, Top Targets, and Threat Map. Each view provides a different perspective on an organization's attack surface.



Figure 1. Attack Dashboard, Threat Entities

## Top Targets

The Attack Dashboard Top Targets view highlights the most frequently targeted sites and endpoints within a tenant. This view is critical for large enterprises with dozens or hundreds of sites protected by the ThreatX Platform. This view puts the most frequently and aggressively targeted sites front and center, allowing administrators to understand their risk profile, and the protection they’re receiving from ThreatX.

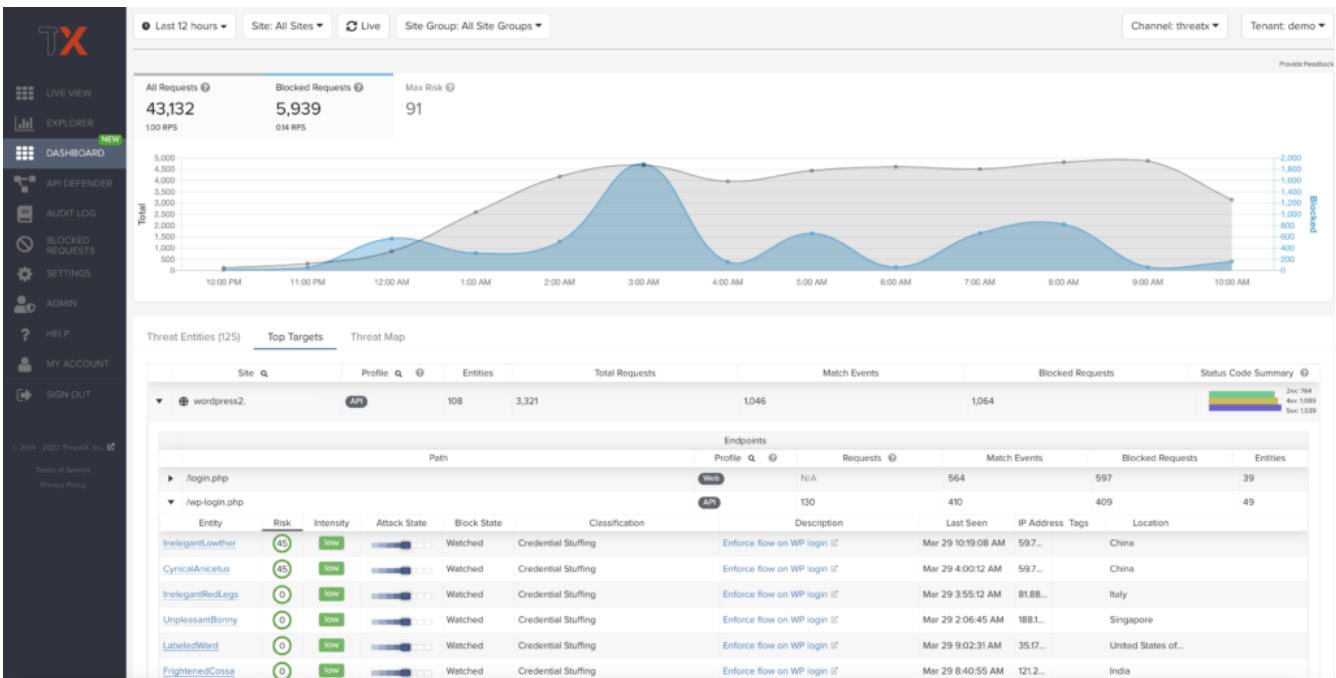


Figure 2. Attack Dashboard, Top Targets

## Threat Map

The Threat Map view, in the Attack Dashboard, provides visibility into the location of each unique entity and its associated risk. The interactive map allows the user to identify how many unique attackers are acting from each country.

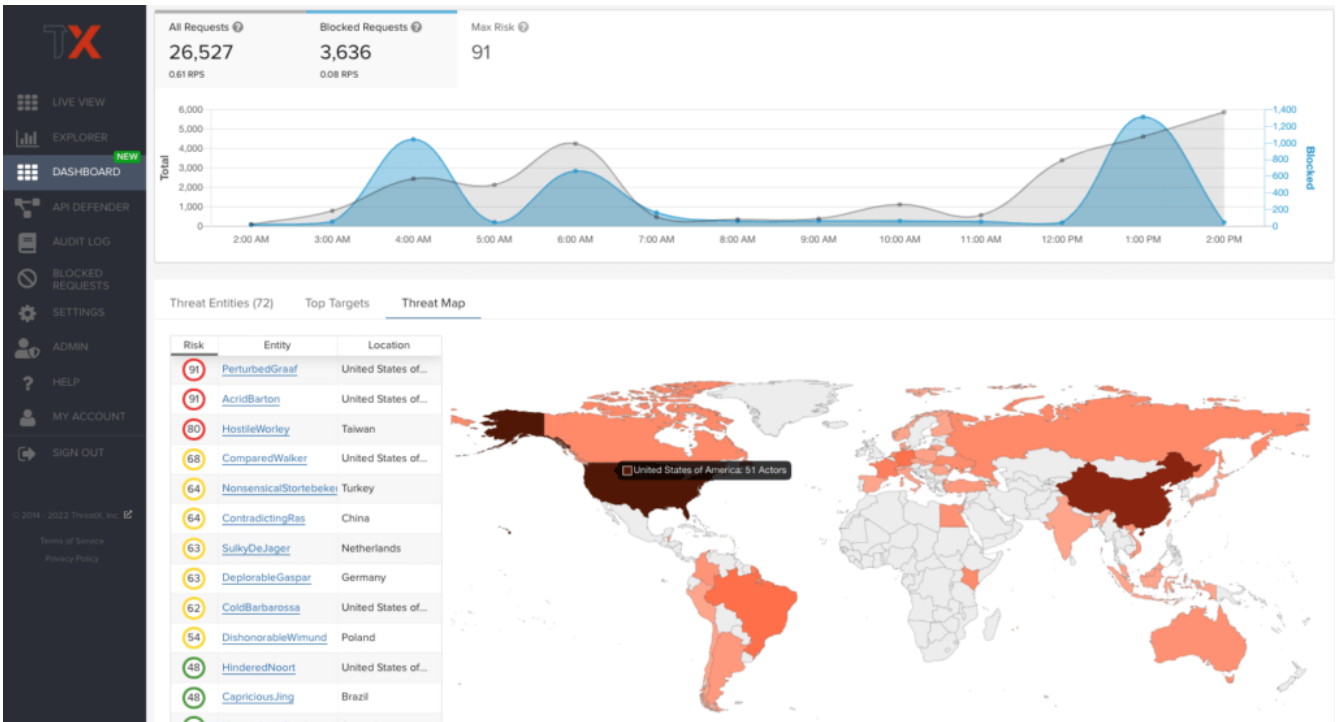


Figure 3. Attack Dashboard, Threat Map

## API Defender

### API Observability

The API Defender dashboard provides visibility into endpoints discovered and protected by the ThreatX platform. API traffic analytics, error code summaries, and visualizations of API schema conformance are displayed in API Defender, as shown below in Figure 4, providing the ability to compare what API traffic is expected vs. an anomaly against your organization’s API specifications. The API Defender dashboard brings together API discovery, observability, and the context needed to understand your organization’s entire attack surface against what is being seen in the wild.

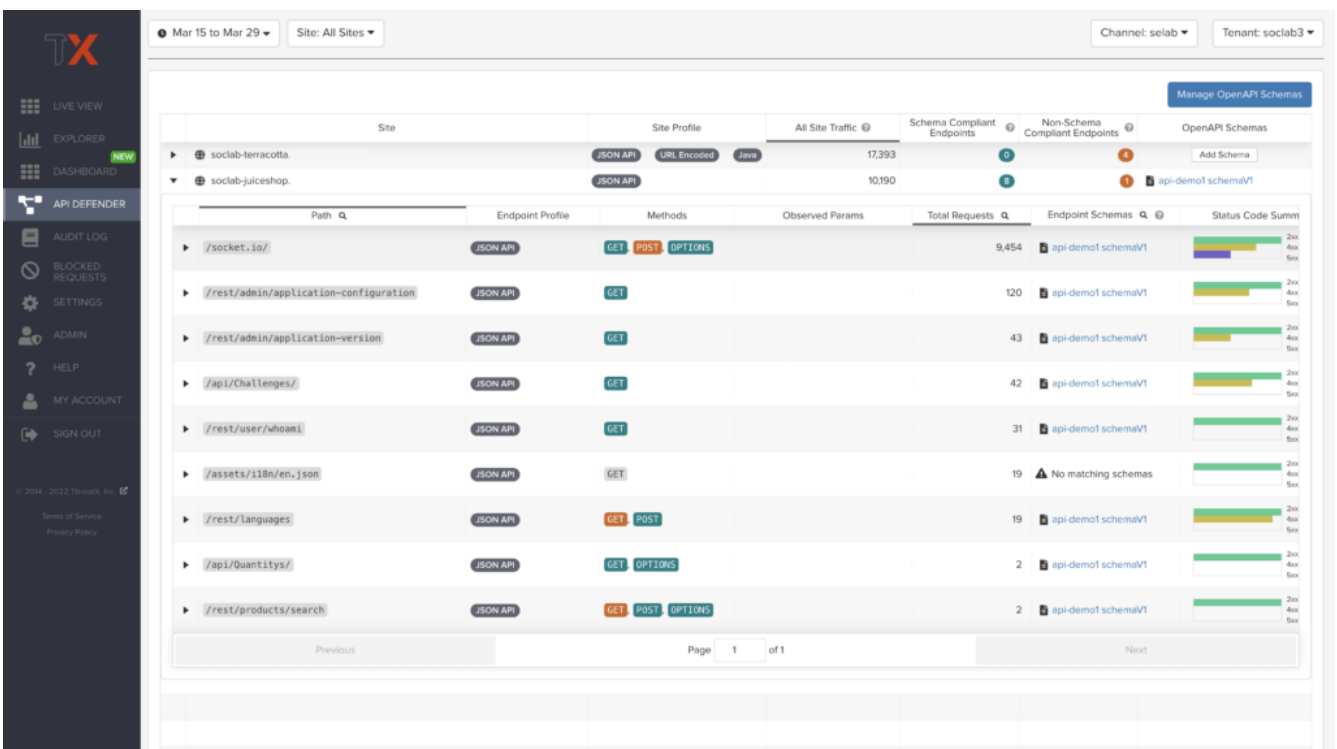


Figure 4. API Defender

## API Discovery

ThreatX's API discovery capabilities analyze and profile legitimate, suspicious, and malicious API use to discover and enumerate the endpoints as well as the traffic they serve. While monitoring API interactions in real-time, ThreatX can accurately detect real API endpoints and determine identifying attributes of their tech stacks or markup encodings.

## Schema Compliance

Schema Compliance gives users the ability to upload, manage, and cross-compare which API traffic is expected according to your organization's schema vs. what is being seen in the wild. Manage your organization's API schemas within the API Defender page to gain risk visibility, simplify schema enforcement, or create API-centered protection rules.

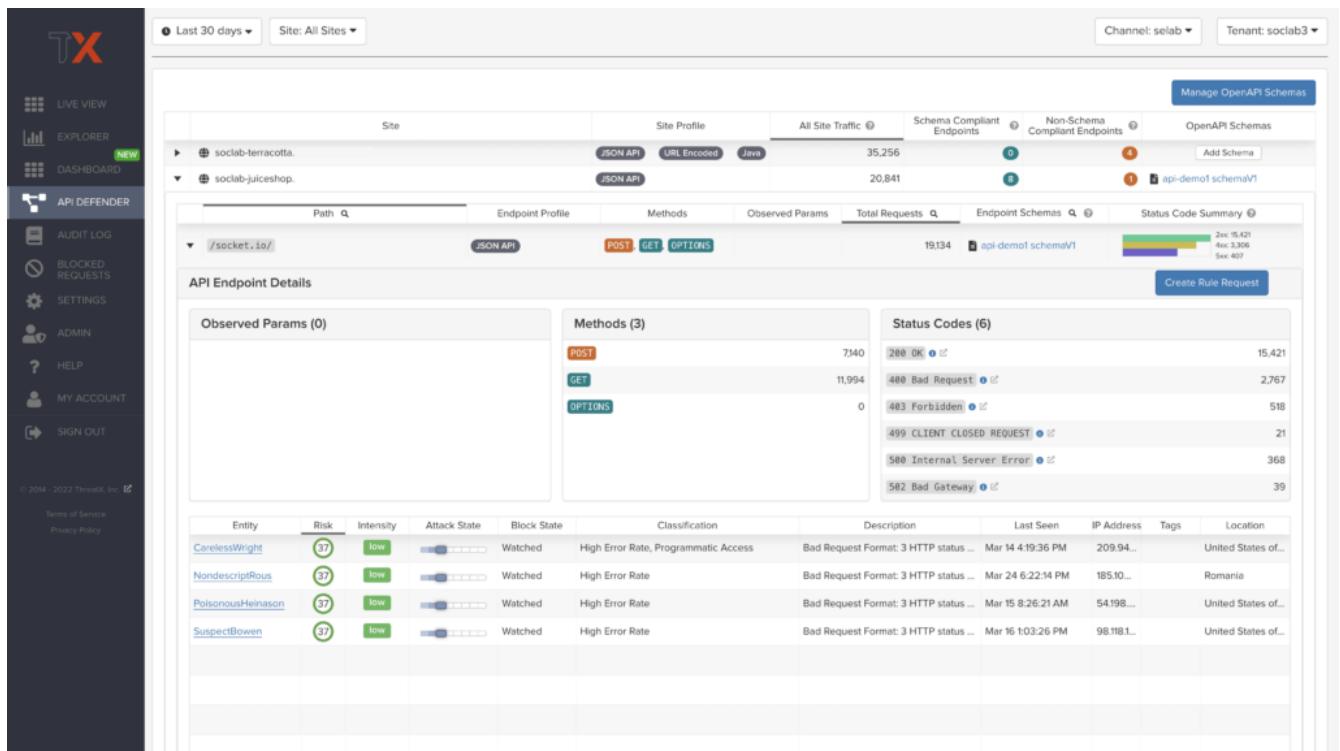


Figure 5. API Defender, Endpoint Details



By default, the ThreatX platform updates the data every few seconds. You can choose to display historical data by selecting a time frame, as described in [Data Controls and Filters](#).

## Common Analytical Tasks

- Monitor changes.
- Review details about a specific threat.
- Determine if traffic from an origin is to be allowed or blocked.
- Identify unexpected usage patterns.

The Dashboard includes graphs and three tables, which are described in the following sections. Each table is a different perspective of the organization's attack surface. For detailed information about the data in the table, see [Managing Threats](#).



## Graphs

The Dashboard includes three interactive graphs.

### Interactive Graphs

#### All Requests

Displays the total number of requests, including benign requests, within the selected time range. It also displays the average number of Requests per Second (RPS). The associated chart displays the number of requests over the selected time range.

#### Blocked Requests

Displays the total number of requests that were blocked within the selected time range. It also displays the average number of RPS. The associated chart displays the number of blocked requests over the time range.

#### Max Risk

Displays the highest system Risk Score recorded during the time range selected. The associated chart displays the maximum Risk Score at each time interval.

You can hover over a point on any graph to display the metrics at that time.

## Threat Entities

The Threat Entities table offers the visibility security teams need to quickly evaluate threats prioritized by the Risk Score and Intensity, which represents the number of times rules were matched over the selected time range.

You can drill into the threat to view specific metadata of that threat, as described in [Entity Details](#).

If you are unfamiliar with the Status icons, you can hover over the icon to see its definition.

## Top Targets

### Top Targets Table Description

*This table focuses on the sites that are most frequently or aggressively targeted by attacks.*

<b>Entities</b>	A column showing the number of threats that targeted the site.
<b>Match Events</b>	A column showing the number of times one or more rules were matched.
<b>Status Code Summary</b>	A field showing the number of responses for each HTTP code and a logarithmic scale to illustrate the relative difference between the numbers.




You can drill-down into a site's endpoints, which are displayed as paths...

## Threat Map

Threat Map offers visibility into the location of each unique threat and its associated risk. The interactive map allows the user to identify how many unique attackers are acting from each country. You can hover over a country on the map, and a pop-up displays the number of attacking threats originating in that country.

## Data controls and filters

The ThreatX dashboard pages offer the following controls and filters that you can use to focus on specific data.

 **Dashboard Pages**

<b>Site group</b>	If your ThreatX platform organizes sites into groups, you can choose which group to view. You can view one site group or all site groups.
<b>Sites</b>	You can display the data for one or all sites.
<b>Tenant</b>	If your ThreatX platform has many tenants and your account has permission, you can choose which tenant to view. You can view one tenant only at a time.
<b>Live</b>	Refreshes the data.
<b>Time range</b>	Choose the time frame to view the data. You can choose a relative time frame, such as the last 12 hours, or an absolute time frame. The time range you select for each page affects the data shown on that page.

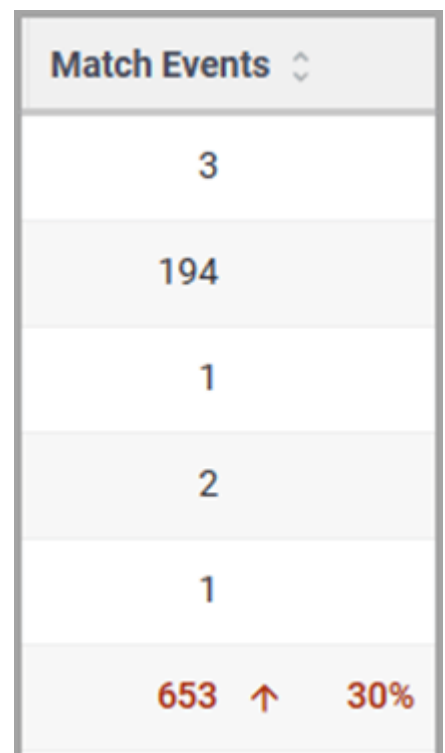
All Site Groups ▾

All Sites ▾

↻ Live

🕒 Last 12 hours ▾

*Figure 6. Dashboard page filters*




*Figure 7. Match event increase of 30%*

Some data in the various tables include a percentage with an arrow. The value indicates a change in the data relative to the baseline reporting period, which is 7 days before the selected time range.

For example, when you select a 12-hour time range, the baseline period is the same 12-hour period from 7 days previous. The arrow indicates an increase or decrease in value. The following figure shows an increase in the number of Match Events of 30%.

## Allow, deny, and block lists

You can use the following lists to always deny, temporarily block, or always allow specific entities. An *entity* is a specific IP address or IP group. A suspicious entity is a threat.

 Lists

<b>Blacklist</b>	Permanently prevents an entities from interacting with any of your sites.
<b>Blocklist</b>	Prevents an entities from interacting with any of your sites for 30 minutes. Request tracking continues during the block period.
<b>Whitelist</b>	Entities on the whitelist are always allowed to interact with your sites.

You can add an entity as an IP address or CIDR to any of the lists manually, as described in [Managing Threats](#). You should exercise caution when manually adding a threat to the Blacklist or Whitelist to prevent a problem with legitimate traffic or always allowing malicious traffic.

If the ThreatX Risk-Based Blocking feature is enabled, the ThreatX platform can add a threat automatically to the Blacklist or Blocklist based on the threat's behavior. The ThreatX behavioral analytics engine, hackerMind™, blocks persistently malicious threats when the threats' behavior surpasses the Risk-Based Blocking threshold. The analytics engine automatically places a threat on the permanent Blacklist after it is blocked three times.

Once added to the Blacklist or Whitelist, the entity remains there permanently until it is manually removed. A user who has Write Access can manually remove an entity from the list, or you can request the ThreatX SOC to remove the entity.

## Entity Details

The ThreatX platform analyzes HTTP traffic then extracts identifying metadata, including IP address, user agent, TLS fingerprint, and other characteristics to create a profile and identifier for each attacker, which is displayed in the Entity Details page. The data is presented with special emphasis on key attributes to further help identify trends and patterns.

The Entity Details page is accessible by clicking a threat on another page, such as the Dashboard.

## Entity Details

100
ComparedJackson

INTENSITY 13
CURRENT STATUS Blacklisted

IP ADDRESS 81.106.11.111

IP REPUTATION 0

LOCATION United Kingdom...

USER AGENT Chrome 115 (Wind...

TAGS Add +

Due to a large amount of data, only match events occurring between Aug 25 8:06:11 AM and Aug 30 4:40:56 AM are loaded into memory. Any sorting or filtering operations will apply only to self subset of event data. If you wish to explore other periods of time, please use the time filter or chart to select an alternate period.

Activity 9472
Responsive Actions ?
Analyst Notes 0
Endpoint Statistics 89

Activity 9472 (1,007 visible) Add Note Download as CSV

Event Metadata					Request Information					
Time	Type	Risk	Blocked	Profile	Domain	Path	Method	User Agent	TLS Fingerprint	P
Aug 30 4:40:56 AM	Rule Match	100	●	API	api.threatx.com	/tx_api/v2/apikeys	POST	Chrome 115 (Windows 10)	23acfb0e1f4755ea65c53f77...	...
Aug 29 5:42:45 AM	Rule Match	100	●	Web	api.threatx.com	/	GET	Go-http-client/1.1	b78f33beadf535ea359eb4c...	...
Aug 29 5:42:45 AM	Rule Match	100	●	Web	api.threatx.com	/	GET	Go-http-client/1.1	b78f33beadf535ea359eb4c...	...
Aug 29 5:42:44 AM	Rule Match	100	●	Web	api.threatx.com	/	GET	Go-http-client/1.1	b78f33beadf535ea359eb4c...	...
Aug 29 5:42:44 AM	Rule Match	100	●	Web	api.threatx.com	/	GET	Go-http-client/1.1	b78f33beadf535ea359eb4c...	...
Aug 29 5:42:44 AM	Rule Match	100	●	Web	api.threatx.com	/	GET	Go-http-client/1.1	b78f33beadf535ea359eb4c...	...
Aug 29 5:42:43 AM	Rule Match	100	●	Web	api.threatx.com	/	GET	Go-http-client/1.1	b78f33beadf535ea359eb4c...	...
Aug 29 5:42:43 AM	Rule Match	100	●	Web	api.threatx.com	/	GET	Go-http-client/1.1	b78f33beadf535ea359eb4c...	...
Aug 29 5:42:43 AM	Rule Match	100	●	Web	api.threatx.com	/	GET	Go-http-client/1.1	b78f33beadf535ea359eb4c...	...

## Metrics

### Metrics - Entity Details

#### Risk Score

#### Threat name

#### Intensity

Represents the number of times rules were matched over the selected time range.

#### Current Status

The current action taken on the threat. You can change the action as needed. .

#### IP Address

If available, you can click the address to see any data about it in the ViewdnsInfo web site.

#### IP Reputation

Represents the legitimacy of the IP address with a score of 0 to 100. The higher the score, the more likely that the IP address is legitimate. A low score can indicate an attacker. A score of 0 could mean that the IP reputation is unknown. The scoring system is the opposite of Risk Score.

#### Location

Country of origin.

#### User agent

The program that sent the request on behalf of the user, such as a web browser or curl, as indicated in the User-Agent header field.

#### Any tags assigned to the threat

If your account has permission, you can add a tag to track similar threats.

## Chart that displays the attacks over time

You can hover over various locations for details of the threat at that time.

## Activity

### Activity - Entity Details

#### Type

If there was an action taken on the request, the column shows the action which can be Watched, Blocked, Whitelisted, or Blacklisted. If there was no action taken, then the Type is Rule Match when the request matches a rule.

#### Risk

Risk Score.

#### Blocked

A red dot indicates that a request from the threat was blocked.

#### Profile

API Profile.

#### Domain

Also referred to as a site.

#### Path

Also referred to as an endpoint.

#### Method

API call used by the threat.

#### TLS fingerprint

Digital certificate fingerprint of the threat.

#### Parameters

URL query parameters of the request, if present.

#### Content-type

Also referred to as an API profile. Content types can be application/json, application/xml or text/xml.

#### Request ID

Random string generated by the ThreatX platform to help identify each request that passes through the ThreatX sensors.

#### Status

HTTP response code unless the threat is blocked.

#### Size

Length of the response in bytes.

#### Time (ms)

Time taken to receive the response from the upstream server.

**Description**

Lists the rules that were matched by the threat. You can click a rule to display the properties for that rule.

**Count**

Number of rules matched by the request.

*Searching*

- You can click the search icon [ 🔍 ] in each column header to filter the table.
- The search icon [ 🔍 ] for some rows will also display a count of each type of entry (e.g., the *Domain* row would show every type of domain and the number of each).

**Active Threats**

If a threat is active, you will see the following changes in the Activity table:

- Additional events with Rule Match in the Type column.
- Increasing Risk Score.
- If your ThreatX platform has the auto-blocking feature enabled, the threat is blocked when it exceeds the auto-blocking threshold and you see a red dot in the Blocked column.

**Blocking**

Blocking is a temporary action and the block is released after a period of time. The Type column changes to Watched. If that entity is still active, you might see more entries with Rule Match. However, some attackers try a few requests, get blocked, give up and do not return.

**Responsive Actions**

The page lists each action taken against the threat.

**Analyst Notes**

The page lists any notes left by an analyst.

You can add a note to give additional data or observations, along with any recommendations or instructions.

**Endpoint Statistics**

The page lists the endpoints that were targeted by the threat. It contains two tables.

- API endpoints table lists the endpoints and their API profile.
- Non-API endpoints table lists the targeted endpoints of non-API sites and the number of rule matches. A *non-API site* is a site not served by an API server. Typically, a non-API site has web assets which are used for human interaction.

The non-API endpoints table might list API endpoints when the ThreatX profiling engine is actively determining if the site is an API or web service site.

## Rule Details

The Rule Details page displays a rule's properties, its conditions, and the actions it takes when the conditions are matched.

[< Back to Rules](#)

### Rule Details ?

Rule ID: 950901

Description ?

Tag Name ?

Classification ?

State ?

Risk ?

Action ?  Track  Block  Tarpit

Visual JSON

Other ?

Delete
Save

### ☐☐ Rule Detail Properties

#### Description

Text that defines the behavior or purpose of the rule.

#### Tag Name

Brief text to identify the rule. The tag exists to identify a rule when a description is long.

#### Classification

Describes the type of attack which the rule assigns to a threat. The classification displays in various tables as the attack class.

#### State

Assigns the threat's assumed objective when the request matched this rule.

#### Risk

Assigns the Risk Level to the attack.

#### Action

The action that the rule performs when responding to a threat. The action appears in the Status column in various tables.

**Track**      Begin or continue tracking a risk score for the offending entity, based on the risk assigned to this rule and other factors.

**Block**      Immediately block the request and track a risk score for the offending entity.

<b>Tarpit</b>	Limit the speed at which the offending entity receives responses and track a risk score for the entity.
<b>Interrogate</b>	Challenge an offending entity with a cookie and try to fingerprint the user-agent.

The **Visual** and **JSON** tabs display the programmatic rule conditions in a Visual or JSON format.

The Rule Details page is accessible from various tables by clicking a rule name in the **Description** column. It is also accessible for the navigation bar by opening **Settings > Rules > <rule details page >** .



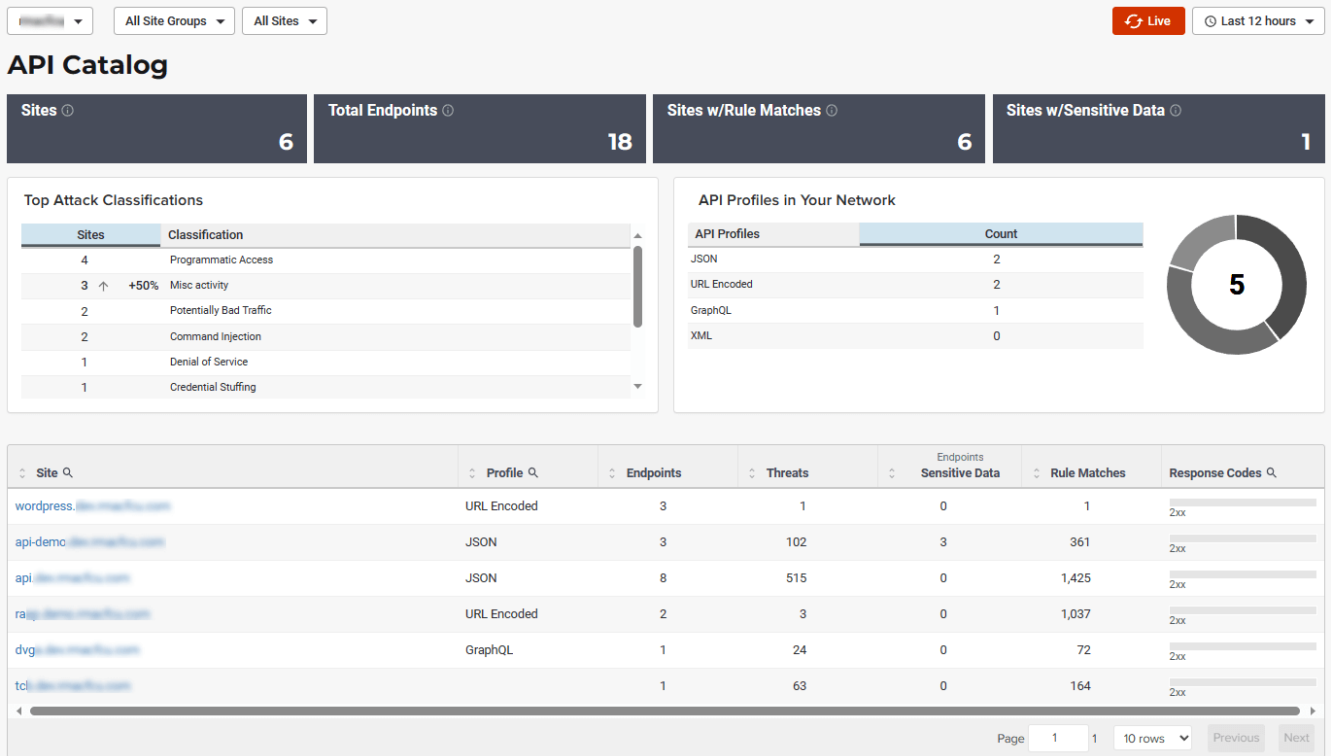
Rule details are read-only unless your account has permission to edit rules.



# API Catalog

## Introduction

The API Catalog displays statistics about the API traffic to the sites in your environment under ThreatX protection. It lists all the known sites, their endpoints, any threats or attacks, type of attack, and the number of times API traffic at a site matched a rule. You can view details about a specific site and then view details about a single endpoint within the site.



If your account has the Sensitive Data feature, the ThreatX platform monitors API responses to detect various data types as shown in the following table. The metrics within the API Catalog indicate the data type, counts and which sites and endpoints are exposing the data.

Table 1. Sensitive Data Classifications

Data Type	Classification
Bearer Token	Authentication Credentials
Credit Card – AMEX	Payment Card Industry Data Security Standard (PCI-DSS)
Credit Card – Diners Club	Payment Card Industry Data Security Standard (PCI-DSS)
Credit Card – Discover	Payment Card Industry Data Security Standard (PCI-DSS)
Credit Card – JCB	Payment Card Industry Data Security Standard (PCI-DSS)
Credit Card – Maestro	Payment Card Industry Data Security Standard (PCI-DSS)
Credit Card – MasterCard	Payment Card Industry Data Security Standard (PCI-DSS)
Credit Card – Visa	Payment Card Industry Data Security Standard (PCI-DSS)
Individual Taxpayer Identification Number (ITIN)	Personally Identifiable Information (PII)
Passport – Next Gen	Personally Identifiable Information (PII)
Social Security Number	Personally Identifiable Information (PII)



- The ThreatX platform reports only sensitive data that is in plain text. It does not report partial or obfuscated data, such as \*--1234.
- The ThreatX platform does not correlate sensitive data with rules or threats or store sensitive data due to security and compliance reasons.



The catalog displays changes over time so that you can determine if there are any trends that need attention.

## Common API Catalog Tasks

- Monitor changes.
- Review details about a specific attack.
- With the Sensitive Data feature, detect sensitive data within API transactions and take appropriate actions.
- Determine if traffic from an origin is to be allowed or blocked.
- Verify that all expected sites are included in the API Catalog.
- Identify unexpected usage patterns.
- Identify endpoints with high error rates.
- Identify endpoints experiencing high levels of attack traffic.
- Request a change to the rules as needed.

Over time, the number of endpoints in the API Catalog might change as the ThreatX API Profiler confirms endpoints or determines that an endpoint was inaccurate. The API Profiler is a function within the ThreatX Sensor that detects, categorizes, and archives API traffic patterns for later analysis within the ThreatX platform.

## Metrics

### API Catalog Metrics

The first row of tiles on the API Catalog page is a quick status for the following metrics:

- Count of **sites in your environment**
- Count of **endpoints**
- Count of **sites with rule matches**
- Count of **sites where sensitive data was exposed** (*requires Sensitive Data feature to be enabled*)
- Count of **API profile types** in your environment.
- Name of the **Attack Class with the highest number of attacks** (*over time*)

### Metrics Table

#### Endpoints, Threats and Rule Matches

Any changes to the number of endpoints or threats with an up or down arrow and the percentage of change.

**Sensitive Data**

The number of endpoints that passed sensitive data. Any change over time is shown as a percentage.

**Threats**

The number of threats, not the number of attacks. A threat can be associated with multiple matched rules. The number of threats is typically smaller than the number of matched rules since one threat can match multiple rules.

**Response Codes**

The number of HTTP responses for each HTTP response code within the selected time range. Hover over the response code bar to see the number of responses per HTTP code. A high count or percentage could indicate that the endpoint is experiencing high levels of invalid input or suffering from elevated error rates. For example, it could represent clients misbehaving, servers being misconfigured, or attempts to exploit software by intentionally exercising unexpected inputs.

## Site Details

You can click a site to see API traffic details for that site. The page focuses on one site and its endpoints and includes the following:

- Rule matches compared to blocked request over time
- Total Blocked requests
- Total Requests
- Sensitive data detections



Any percentages are change over time.

## Endpoint Details

You can click an endpoint to see API traffic details for that endpoint. The page displays data specific to one endpoint.

The navigation bar includes all the endpoints and number of rule matches. You can navigate to different endpoints to view their details.

### Endpoint Details Tables

**Traffic Trends**

List of metrics for the endpoint along with the percentage of change of the requests within the selected time range.

**Response Code Trends**

HTTP response codes, number of times they occurred within the selected time range, and the percentage change.

**Sensitive Data**

This table shows the type of sensitive data detected in the endpoint, number of times they occurred within the selected time range, and the percentage change. The Data Type shows the type of data, such as credit card, social security number, or credentials.

## Threats

This table gives details about the threats for that endpoint. You can click a threat name to open its [Entity Details](#) page. You can also click a rule name to see the activity of that rule.



If you see traffic that should be monitored, click **Request a Rule** to request that the ThreatX SOC write a rule for a specific situation.