

threatER Portal User Guide, June 2024

Collect	4
Lists	4
List Types	5
Allow Lists	5
Block Lists	6
Threat Lists	6
List Creation	7
Creating IP Threat Lists	7
Creating Manual IP Allow & Block Lists	7
List Details	7
Add Entries	8
Apply to Policies	11
Create New Policy During List Creation	11
Creating Manual Domain Lists	12
List Details	12
Add Entries	13
Adding & Removing Manual List Entries	15
Editing all List Components	18
Deleting a List	20
Enforce	22
Enforcers	22
Enforce Configuration	24
Settings	24
Syslog	26
Access	27
Bridges	29
NTP	29
Enforce Software	33
Update Now	34
Schedule Update	35
Cancel a Scheduled Update	36
Revert to Previous Build	37
Manual Downloads	39
Subscription Management	39
Editing Enforcer Name and Location	41
Subscription Throughput	41
Networks	42
Creating Networks	43
Network Details	43

Inbound/Outbound	44
Create New Policy During Network Creation	46
IPs	46
Editing a Network	48
Deleting a Network	50
Ports	51
Adding Ports	51
Editing Ports	53
Deleting Ports	53
Policies	54
Create a Policy	54
Policy Details	55
IPs by Country	55
Reserved and Unassigned IPs	57
IPS by ASN	57
Risk Thresholds	58
Best Practice Recommendation for Risk Thresholds:	60
Lists	61
Best Practice Recommendation for Lists:	61
Creating an Allow All Policy	62
Edit a Policy	62
Delete a Policy	63
Subscriptions	64
Unexpected Blocks	66
Reports	69
Allowed/Blocked	70
Reason Summary	71
Category Summary	73
Top 10 Countries	74
Top 10 ASNs	75
Тор 10	77
Countries by Threat Category	77
ASNs by Threat Category	77
Scheduled Reports	78
Editing Scheduled Reports	80
Disabling Scheduled Reports	82
Deleting Scheduled Reports	82
Marketplace	84
Included with Enforce Products	84
Premium Intelligence Products	85

Services	86
Administration	87
Users	87
Create New User	87
Edit User Accounts	88
Disable an Account	688
Enable an Account	89
Update User Email	90
Update User Role	90
Update User Password	91
Delete Users	92
Users Filter	92
Subscriptions	93
Command Logs	93
IOC Search	94
User Profile	95
User Details	95
API Key	96
Multi-Factor Authentication (MFA)	96
MFA for Individual Account	96
Deactivate MFA	97
MFA Required by Company	98
Company Profile	99
Single Sign-On (SSO)	100
API	101
Multi-Factor Authentication (MFA)	102
Appendix	103
User Roles and Permissions	103
User Management	106

Collect

Collect is threatER's centralized SaaS solution to aggregate all of your threat intelligence. Collect provides customers access to best-in-class cyber intelligence feeds and threat lists, as well as the ability to create their own lists.

Lists

All List Types – Allow, Block, Threat – are consolidated into one table that is accessible by selecting Collect from the left-hand navigation and then selecting the Lists tab.

= threater									Q (?) (8)
E Collect	•								
➢ Enforce		LISTS					MARKE	TPLACE	
合 Marketplace	Lists (1-20 of 37 total)								Create
4 Messages	All Types 👻	All Health States	- All Indicat	ors -	All Sources	•	All Access	✓ Reset Filter	٩
Administration	NAME 🗇	TYPE 😄 INDICATOR 🖨	SOURCE 🖨		es 😄 count 🖨	LAST SYNC 👙	LAST UPDATE 🖨	DESCRIPTION	G
{} API Docs	Akamai	Allow	CSV File Connector	Public None	19	10/25/23, 02:00 PM	02/13/23, 04:44 PM	Akamai curated by Greynoise	1
	Amazon Cloudfront	Allow	CSV File Connector	Public None	144	10/25/23, 02:02 PM	07/10/23, 05:56 PM	Amazon Cloudfront curated by Greynoise	:
	Bambenek ML-Malware	Block Domain	Bambenek	Public None	2,672	10/25/23, 02:14 PM	10/25/23, 02:14 PM	Machine Learning - Malware Domain feed	:
	Bambenek ML-Phishing	Block Domain	Bambenek	Public None	5,426	10/25/23, 01:29 PM	10/25/23, 01:29 PM	Machine Learning - Phishing Domain feed	
	Bitdefender APT-Domains	Block Domain	Bitdefender	Public None	11,042	10/25/23, 01:51 PM	10/25/23, 01:51 PM	Dec 20 2.23 pm	
	Bitdefender C2-IPs	Block	Bitdefender	Public None	718	10/25/23, 02:00 PM	10/25/23, 02:00 PM	Bitdefender Command and Control (C2) IPs F	eed
	Bitdefender Malicious-do	Block Domain	Bitdefender	Public None	401,593	10/25/23, 01:54 PM	10/25/23, 01:54 PM	Dec 20 2.23 pm	1

The table contains the following details on each List Type:

- List Name
- Health State
 - Healthy if a list is in this state, a green pip will display to the left of the list name
 - Needs Attention if a list needs attention, a red pip will display to the left of the list name.
 When a list is in this state, the configuration of the list should be checked to ensure all settings are correct.
- Indicator will display the Indicators contained in the list (IP or Domain)
- Source
 - Manual will display for all Manual Lists that were created
 - For any plugin or integration, the Source Name or Type will display (ex. Basic HTTP, CSV File Connector, etc.)

- Access
 - Private indicates the List was created by the end user. Private lists are editable and can be deleted by the end user
 - Public indicates the List is not owned or managed by the end user and cannot be edited or deleted by the end user
- Count Indicates the number of entries (IPs or Domains) in the List
- Last Sync This is the last time threatER connected to the 3rd party system to check for updates to the list. For Manual Lists, this will display the date the list was last edited
- Last Update This is the last time the content of the list was modified
- Description

Users can filter down the results in the Lists table by utilizing the filter drop-downs and text filter above the table.

List Types

Allow Lists

Allow Lists can be used to ensure that trusted IPs and Domains are always allowed by Enforce, even in the case where your policies would otherwise block the connection due to country, ASN, threat list, or block list.

As Enforce can handle up to 150 million unique threat indicators with 10–30 million indicators provided out of the box, it is possible that users will run into outbound or inbound connections being blocked unexpectedly. Users can manage these blocked connections by configuring Allow Lists either utilizing manual lists or plugins. Unlike many other security controls on the market, there are no limits to the amount of entries you can include in your lists.

PLEASE NOTE:

- Both Allow IP and Domain lists are enabled on a **per-policy** basis.
- If you are unable to enable domain lists per policy, please make sure your Enforcers all have the latest Enforce software installed. If any Enforcer is running a version previous to Enforce Build 214, please update immediately to enable domain lists on a per-policy basis.

Block Lists

Block Lists can be used to ensure that known-malicious IPs and Domains are blocked by Enforce.

PLEASE NOTE:

- Both Block IP and Domain lists are enabled on a **per-policy** basis.
- If you are unable to enable domain lists per policy, please make sure your Enforcers all have the latest Enforce software installed. If any Enforcer is running a version previous to Enforce Build 214, please update immediately to enable domain lists on a per-policy basis.

Out-of-the-box partner block lists provided by threatER are refreshed at regular intervals. Depending on the rules enforced by the partner feed, the update interval can be anywhere from immediate, to every few minutes, to once per hour, and so on.

Threat Lists

Threat Lists are provided by our partners Webroot (included with your Enforce subscription) and Proofpoint (available in our Marketplace). These lists are composed of 3 pieces of information:

- IP Address where an identified threat originates from
- Category what type of threat has been identified
- Score a confidence score ranging from 1 to 100 where 1 is least likely to be a threat, and 100 is most likely to be a threat

Threat Lists are used in Policy Risk Thresholds.

PLEASE NOTE:

- Threat lists are enabled on a **per-policy** basis.
- If you are unable to enable threat lists per policy, please make sure your Enforcers all have the latest Enforce software installed. If any Enforcer is running a version previous to Enforce Build 214, please update immediately to enable domain lists on a per-policy basis.

Out-of-the-box Threat Lists are refreshed per terms of the partner feed, which is generally every few minutes.

List Creation

Creating IP Threat Lists

Currently, threatER does not support Manual Threat Lists, or Threat Domain lists. The application does support the following Threat IP Plugins:

- Threat IP CSV File Connector
- <u>Anomali</u>

Creating Manual IP Allow & Block Lists

To create a manual IP list:

- Navigate to Collect in the left-hand navigation menu
- Select the Lists tab
- Select the "Create" button in the top-right corner

= threater									<u> २</u> ७ ७
Collect		LISTS					MARKE	TPLACE	
 ➢ Enforce ☆ Marketplace 	Lists (1-20 of 37 total)								Create
🕂 Messages	All Types -	All Health States	✓ All Indica	tors •	All Sources	*	All Access	- Reset Filter	Q
Administration	NAME 🗘	TYPE 🗇 INDICATOR	SOURCE 🖨	ACCESS 🔅 POLIC	CIES 😄 COUNT 🖨	LAST SYNC 👙	LAST UPDATE 👙	DESCRIPTION 🐡	G⁺
{} API Docs	Akamai	Allow	CSV File Connector	Public None	19	10/25/23, 02:00 PM	02/13/23, 04:44 PM	Akamai curated by Greynoise	
	Amazon Cloudfront	Allow	CSV File Connector	Public None	144	10/25/23, 02:02 PM	07/10/23, 05:56 PM	Amazon Cloudfront curated by Greynoise	

List Details

Provide the following (* indicates required field):

- *Name (unique name required)
- *Source
 - Select Manual from the drop-down
- *List Type
 - Select Allow or Block from the drop-down
 - Note: Manual Threat Lists (IP & Domain) are not supported at this time
- *Indicator

- Select IP from the drop-down
- Description

Once all required fields are complete, select the Next button to proceed to the Add Entries step.

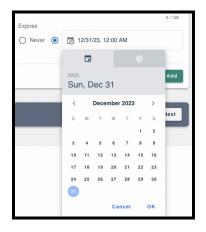
Create List		
Lists can be used to allow or block IPs and Domains.	The indicators contained in the list will be blocked or allowed, depending on the list type, per the Polic	cy it is assigned to.
1 LIST DETAILS	add entries	3 APPLY TO POLICIES
Manual IP Allow List Details		
Customer IP Allow List	Source Manual	•
	22 / 64	
List Type Allow	- IP	•
Description		
List of IPs to Allow		
		20 / 128
		Next

Add Entries

To add entries to the list, enter the following (* indicates required field):

- *IP address
- *Maskbits
- Description (optional)
- *Expiration
 - Default expiration is set to "Never"
 - To provide an expiration date and time:
 - Select the radio button next to the timestamp field
 - Select a date from the calendar

ó





- Click on the clock tab and move the dial to the hours setting that is desired
- Move the dial to the minutes setting that is desired and click OK



• Select the Add button to add the IP to the list

LIST DETAILS	2 ADD ENTRIES		(3) Apply to policies
IP List		Remove	Create IP Clear
IP IP	MASKBITS EXPIRES DESCRIPTION		IP 1.2.3.4
	Add IPs to this List To add an IP to this list, enter the IP address, maskbits, optional expiration date and click Add.		Maskbits 32
			Description
			0/128 Expires ○ Never
			Add

• Follow the steps above to add additional IPs to the list

Once all IPs are added, select the Next button to proceed to the Apply to Policies step.

LIST	V T DETAILS			2 ADD ENTRIES		(3) APPLY TO POLICIES
IP List	t			R	Create IP	Clear
	IP	MASKBITS	EXPIRES	DESCRIPTION	IP	
	1.2.3.4	32	12/31/23, 12:30 PM			
	2.3.4.5	32	-		Maskbits 32	٥
	3.4.5.6	32	-	-		
	4.5.6.7	32	01/31/24, 12:30 PM		Description	
					Expires	0 / 128
					🔿 Never 💿 🐻 01/31/24,	12:30 PM
						Add
Prev	vious					Next

NOTE: To remove an entry before moving to the next step, select the checkbox next to the entry and select the Remove button.

Apply to Policies

Entries within an IP list are not allowed or blocked until the List is applied to a Policy. To apply this new list to a policy, select the applicable policies. Once all desired selections are made, select the Create List button to create the List.

LIS	♥ ST DETAILS	ADD ENTRIES		3 APPLY TO POLICIES
Apply	v to Policies		Filter	Q New Policy
	NAME	DESCRIPTION		
	Inbound	all inbound traffic		
	Outbound	all outbound traffic		
			PER PAGE: 20 👻	1-2 total < PREVIOUS 1 NEXT >
Pre	vious			Create List

Create New Policy During List Creation

If a policy does not exist that you want to apply your list to, you have the option to create a new policy within the Create List wizard. To do so, select the "New Policy..." button on the Apply to Policies step and then follow the steps to create a policy, outlined above in the Policies section of this document.

LIST DETAILS	ADD ENTRIES	3 APPLY TO POLICIES
Apply to Policies		Filter Q New Policy
NAME	DESCRIPTION	
✓ Inbound	all inbound traffic	
Outbound	all outbound traffic	
		PER PAGE: 20 V 1-2 total < PREVIOUS 1 NEXT >
Previous		Create List

۲

Creating Manual Domain Lists

To create a manual Domain list:

- Navigate to Collect in the left-hand navigation menu
- Select the Lists tab
- Select the "Create" button in the top-right corner



		LISTS						MARKE	TPLACE	
Lists (1-20 of 38 total) All Types	All Healt	h States	 All Indica 	itors	•	II Sources	•	All Access	✓ Reset Filter	Create Q
NAME 🖨	TYPE 🖨		SOURCE 🖨	ACCESS	POLICIES	COUNT 🖨	LAST SYNC	LAST UPDATE 🚔		G
Akamai	Allow	IP	CSV File Connector	Public	Inbound	19	10/30/23, 02:59 PM	02/13/23, 04:44 PM	Akamai curated by Greynoise	:
Amazon Cloudfront	Allow	IP	CSV File Connector	Public	Inbound	144	10/30/23, 03:01 PM	07/10/23, 05:56 PM	Amazon Cloudfront curated by Greynoise	:
Bambenek ML-Malware	Block	Domain	Bambenek	Public	None	3,117	10/30/23, 03:13 PM	10/30/23, 03:13 PM	Machine Learning - Malware Domain feed	
Bambenek ML-Phishing	Block	Domain	Bambenek	Public	None	5,245	10/30/23, 03:29 PM	10/30/23, 03:29 PM	Machine Learning - Phishing Domain feed	
Bitdefender APT-Domains	Block	Domain	Bitdefender	Public	None	11,106	10/30/23, 02:50 PM	10/30/23, 02:50 PM	Dec 20 2.23 pm	

List Details

Provide the following (* indicates required field):

- *Name (unique name required)
- *Source
 - Select Manual from the drop-down
- *List Type
 - Select Allow or Block from the drop-down
 - Note: Manual Threat Lists (IP & Domain) are not supported at this time
- *Indicator
 - Select Domain from the drop-down
- Description
- To Enable this list globally for all policies, position the Enabled toggle (above the Name field) to the right (the toggle will turn blue)

Once all required fields are complete, select the Next button to proceed to the Add Entries step.

Create List	
Lists can be used to allow or block IPs and Domains. The indicators contained in the list will be b	blocked or allowed, depending on the list type, per the Policy it is assigned to.
1 LIST DEYAILS	add entries
Manual Domain Block List Details	
Name Customer Manual Domain List	Source Manual
27/64	
List Type Block ~	Indicator Domain ~
- Description List of domains to block	
	24 / 128
	Next

Add Entries

To add entries to the list, enter the following (* indicates required field):

- *Domain
- Description (optional)
- *Expiration
 - Default expiration is set to "Never"
 - To provide an expiration date and time:
 - Select the radio button next to the timestamp field
 - Select a date from the calendar

Expires								0 / 128	
🔿 Never 🧿	1	2/31							
	²⁰²³ Sur	2023 Sun, Dec 31							
_	< December 2023 >								
	S	м	т	W	т	F	S	lext	
_						1	2		
	3	4	5	6	7	8	9		
	10	11	12	13	14	15	16		
	17	18	19	20	21	22	23		
	24	25	26	27	28	29	30		
	31								
				Ca	ncel		ок		



Click on the clock tab and move the dial to the hours setting that is desired

•

• Move the dial to the minutes setting that is desired and click OK



• Select the Add button to add the Domain to the list

Create List	w or block IPs and Domains. The indic	ators contained in the list will be blocked (or allowed, depending on	the list type, per the Policy it is assigned	to.
LIST DETAILS					2 ADD ENTRIES
Domain List			Remove	Create Domain	Clear
DOMAIN	EXPIRES	DESCRIPTION		Domain unwanted.com	
	Add Domair To add a Domain to this list, enter the Don	IS to this List		Expires	M
Previous					Create List

- Follow the steps above to add additional Domains to the list
- One all domains are added, select the Next button
- Select the checkbox(es) next to the policy(s) you would like the list enabled on

lists can be used to allow or block IPs and Don	ains. The indicators contained in the list will be blocked or allowed, depen	ding on the list type, per the Policy it is ass	signed to.
LIST DETAILS	ADD ENTRIES		3 APPLY TO POLICIE
pply to Policies		Filter	Q New Policy
NAME	DESCRIPTION		
Inbound	all inbound traffic		
Outbound	all outbound traffic		
		PER PAGE: 20 ♥ 1-2 t	otal < PREVIOUS 1 NEXT

Select the Create List button to create the List.

Adding & Removing Manual List Entries

To add entries to a Manual List:

- Select the applicable List type (Allow or Block) from the filter at the top of the table
- Find the list in the table and click on the list name

	LISTS							MARKETPLACE				
Lists (1-20 of 21 filtered. 38 total)	Lists (1-20 of 21 filtered. 38 tota) Create											
Block	All Health St	ates	✓ All Indicators		▼ All Se	ources	•	All Access	• Reset Filter	Q		
NAME 😄	туре 🖨		SOURCE	ACCESS	POLICIES	COUNT 🖨	LAST SYNC	LAST UPDATE	DESCRIPTION	G		
Bambenek ML-Malware	Block	Domain	Bambenek	Public	None	3,117	10/30/23, 03:13 PM	10/30/23, 03:13 PM	Machine Learning - Malware Domain feed			
Bambenek ML-Phishing	Block	Domain	Bambenek	Public	None	5,245	10/30/23, 03:29 PM	10/30/23, 03:29 PM	Machine Learning - Phishing Domain feed			
Bitdefender APT-Domains	Block	Domain	Bitdefender	Public	None	11,109	10/30/23, 03:51 PM	10/30/23, 03:51 PM	Dec 20 2.23 pm			
Bitdefender C2-IPs	Block	IP	Bitdefender	Public	None	792	10/30/23, 02:59 PM	10/30/23, 02:59 PM	Bitdefender Command and Control (C2) IPs Feed			
Bitdefender Malicious-do	Block	Domain	Bitdefender	Public	None	398,279	10/30/23, 03:11 PM	10/30/23, 03:11 PM	Dec 20 2.23 pm			
Bitdefender Phishing-dom	Block	Domain	Bitdefender	Public	None	248,620	10/30/23, 02:57 PM	10/30/23, 02:57 PM	Dec 20 2.24 pm			
Blocklist.de	Block	IP	Basic HTTP	Public	Inbound +1	23,130	10/30/23, 03:05 PM	10/30/23, 03:05 PM				
CINS Army list	Block	IP	Basic HTTP	Public	 Inbound +1 	15,000	10/30/23, 03:05 PM	10/30/23, 03:05 PM				
CISA Alert List	Block	IP	CSV File Connector	Public	 Inbound +1 	399	10/30/23, 03:05 PM	10/30/23, 03:05 PM				
Cloud Attackers	Block	IP	CSV File Connector	Public	None	15,533	10/30/23, 03:19 PM	10/30/23, 03:19 PM				
Customer Manual Domain L	Block	Domain	Manual	Private	None	1	10/30/23, 03:52 PM	10/30/23, 03:52 PM	List of domains to block	:		
Cyjax	Block	IP	Cyjax	Public	None	58	10/30/23, 03:18 PM	10/30/23, 11:14 AM				
Cyjax	Block	Domain	Cyjax	Public	None	255	10/30/23, 03:11 PM	10/30/23, 11:07 AM	Cyjax Threat Intelligence Feed			

- In the Search field, enter the IP or Domain to add
- If the entry does not already exist in the list, click the "+" sign in the right hand corner

		LISTS		MARKETPLACE						
List Cus	tomer Manual Domair	n List					Ō /			
List of dom	ains to block									
List Details										
LIST TYPE Block	INDICATOR Domain	SOURCE	ACCESS Private	POLICY None	COUNT 1	LAST SYNC 10/30/23, 03:52 PM	LAST UPDATE 10/30/23, 03:52 PM			
Domain Lis	st (1-0)					anotherunwanted.com	· ⊗ < ī ⊕			
DOMA	IN	INSERTED		EXPIRES	1	DESCRIPTION				
			No Ent	ries to Display						
						PER PAGE: 20	<pre></pre>			

• In the right-hand panel, enter the applicable data and click the "Add' button"

Domain List (1-0)			anotherunwanted.com	۹	Create Domain Clear
DOMAIN	INSERTED	EXPIRES	DESCRIPTION		Domain anotherunwanted.com
		No Entries to Display			Expires () [10/30/23, 04:00 PM]
			PER PAGE: 20 👻	< PREVIOUS NEXT >	•
					Cancel

Follow the steps above to add additional entries to the list.

To remove entries from a Manual List:

- Select the applicable List type (Allow or Block) from the filter at the top of the table
- Find the list in the table and click on the list name

	LISTS						MARKETPLACE					
Lists (1-20 of 21 filtered. 38 total)										Create		
Block	- All Health St	ates	✓ All Indicators		✓ All Sc	ources	•	All Access	✓ Reset Filter	Q		
NAME 🌐	түре 🌐		SOURCE	ACCESS	POLICIES	COUNT 🖨	LAST SYNC	LAST UPDATE 👙	DESCRIPTION	F		
Bambenek ML-Malware	Block	Domain	Bambenek	Public	None	3,117	10/30/23, 03:13 PM	10/30/23, 03:13 PM	Machine Learning - Malware Domain feed			
Bambenek ML-Phishing	Block	Domain	Bambenek	Public	None	5,245	10/30/23, 03:29 PM	10/30/23, 03:29 PM	Machine Learning - Phishing Domain feed			
Bitdefender APT-Domains	Block	Domain	Bitdefender	Public	None	11,109	10/30/23, 03:51 PM	10/30/23, 03:51 PM	Dec 20 2.23 pm			
Bitdefender C2-IPs	Block	IP	Bitdefender	Public	None	792	10/30/23, 02:59 PM	10/30/23, 02:59 PM	Bitdefender Command and Control (C2) IPs Feed			
Bitdefender Malicious-do	Block	Domain	Bitdefender	Public	None	398,279	10/30/23, 03:11 PM	10/30/23, 03:11 PM	Dec 20 2.23 pm			
Bitdefender Phishing-dom	Block	Domain	Bitdefender	Public	None	248,620	10/30/23, 02:57 PM	10/30/23, 02:57 PM	Dec 20 2.24 pm			
Blocklist.de	Block	IP	Basic HTTP	Public	 Inbound +1 	23,130	10/30/23, 03:05 PM	10/30/23, 03:05 PM				
CINS Army list	Block	IP	Basic HTTP	Public	 Inbound +1 	15,000	10/30/23, 03:05 PM	10/30/23, 03:05 PM				
CISA Alert List	Block	IP	CSV File Connector	Public	 Inbound +1 	399	10/30/23, 03:05 PM	10/30/23, 03:05 PM				
Cloud Attackers	Block	IP	CSV File Connector	Public	None	15,533	10/30/23, 03:19 PM	10/30/23, 03:19 PM				
Customer Manual Domain L	Block	Domain	Manual	Private	None	1	10/30/23, 03:52 PM	10/30/23, 03:52 PM	List of domains to block	:		
• Сујах	Block	IP	Cyjax	Public	None	58	10/30/23, 03:18 PM	10/30/23, 11:14 AM				
Cyjax	Block	Domain	Cyjax	Public	None	255	10/30/23, 03:11 PM	10/30/23, 11:07 AM	Cyjax Threat Intelligence Feed			

- Select the checkbox(es) next to the entry(ies) that should be removed
- Select the Trash icon

Domain List (1-2 of 2)			Search Q 🛅 🛨
DOMAIN	INSERTED	EXPIRES	DESCRIPTION
anotherunwanted.com	10/30/23, 04:01 PM	-	
unwanted.com	10/30/23, 03:52 PM	01/31/24, 12:29 PM	- / /
			PER PAGE: 20 - 1-2 total < PREVIOUS 1 NEXT >

• On the confirmation modal, select the Delete button

Delete List Entries	
Are you sure you want to Delete this List Entry?	
unwanted.com	
Cancel	Delete

The entries are now deleted from the list.

Editing all List Components

To edit all components (details, entries, policies) of a Manual list :

• Find the List in the table and from the the ellipsis menu, select Edit

Lists (15 filtered. 39 total))											Create
Block	- A	II Health States	▼ IP		→ AI	Sources	*	All Access	.	Reset	Filter	Q
NAME 🖨	TYPE 🖨		SOURCE	ACCESS	POLICIES	COUNT 🖨	LAST SYNC	LAST UPDATE	DESCRIPTION			G
Bitdefender C2-IPs	Block	IP	Bitdefender	Public	None	795	10/31/23, 03:23 PM	10/31/23, 03:23 PM	Bitdefender Comn	nand and Cor	ntrol (C2) IPs Feed	:
Blocklist.de	Block	IP	Basic HTTP	Public	Inbound +1	23,204	10/31/23, 02:28 PM	10/31/23, 02:28 PM	-			0 0 0
CINS Army list	Block	IP	Basic HTTP	Public	Inbound +1	15,000	10/31/23, 02:28 PM	10/31/23, 02:28 PM	-			0 0 0
CISA Alert List	Block	IP	CSV File Connector	Public	Inbound +1	399	10/31/23, 02:28 PM	10/31/23, 02:28 PM	-			0 0 0
Cloud Attackers	Block	IP	CSV File Connector	Public	None	15,269	10/31/23, 02:42 PM	10/31/23, 02:42 PM	-			:
Customer Manual List -	Biuck	IP.	Manual	Private	Inbound +1	2		10/31/23, 03:23 PM	-		Edit	:
Cyjax	Block	IP	Cyjax	Public	None	49	10/31/23, 02:41 PM	10/30/23, 11:14 AM			Delete	:
DHS Information Sharing	Block	IP	DHS Combined	Public	Inbound +1	0	10/31/23, 03:23 PM	06/18/23, 07:02 AM	DHS Information S	Sharing		:



- Edit List Details -
 - This Is the default view when editing a list. Make any necessary edits and then select another step that requires updates. If edits are only needed on this step, select the Save button in the top right corner

Edit List Customer Manual List Lists can be used to allow or block IPs and Domains. The in	ndicators contained in the list will be blocked or allowed, depending on the list type, per the Polic	Cancel Save
LIST DETAILS	ENTRIES	APPLY TO POLICIES
Manual IP Block List Details Name Customer Manual List	- Source Manual	
C List Type	20/64	
Block	v IP	•
Description		
		0 / 128

- Edit Entries -
 - Select this step to add or remove entries
 - Refer the Adding & Removing Manual List Entries section for guidance on how to amend existing list entries
 - If no other List edits are desired, select the Save button in the top right corner
 - If additional List edits are needed, select the applicable step

Edit	Edit List Customer Manual List										
Lists	can be used to	allow or block IPs and Domains. The i	ndicators contained in th	e list will be blocked or allowed, depending or	n the list type, per the Policy it is assig	gned to.					
u	ST DETAILS			entries		APPLY TO POLICIES					
Man	ual Block IP Lis	st (1-2 of 2)			Search	۹ 🗇					
	IP 🔺	MASKBITS	INSERTED	EXPIRES	DESCRIPTION						
	1.2.3.4	32	10/31/23, 03:23 PM	-	-	Î					
	2.3.4.5	32	10/31/23, 03:23 PM	-		ĵ					
					PER PAGE: 20 1-2 tot	al < previous 1 Next >					

- Apply to Policies
 - Select this step to adjust the Policies the List should apply to
 - Refer to the Apply to Policies section above for guidance
 - If no other List edits are desired, select the Save button in the top right corner

Edit	List Customer Manual List			Cancel Save
Lists	can be used to allow or block IPs and Domains. The indicators contained	in the list will be blocked or allowed, depending on the list type, per the f	Policy it is assigned to.	
LIS	O T DETAILS	entries		APPLY TO POLICIES
Apply	to Policies		Filter	Q
	NAME	DESCRIPTION		
	Inbound	all inbound traffic		
	Outbound	all outbound traffic		
		PER PAGE:	20 👻 1-2 total < PR	EVIOUS 1 NEXT >

NOTE: Lists that are tagged as "Public" Access cannot be edited by end users.

Deleting a List

To delete a List:

• Find the List in the table and from the the ellipsis menu, select Delete

Block	→ Al	I Health States	▼ IP		▼ AI	I Sources	*	All Access	*	Reset	Filter	Q
AME 🐡	түре 🖨		SOURCE	ACCESS	POLICIES	COUNT 🖨	LAST SYNC	LAST UPDATE	DESCRIPTION			G
Bitdefender C2-IPs	Block	IP	Bitdefender	Public	None	795	10/31/23, 03:23 PM	10/31/23, 03:23 PM	Bitdefender Comma	and and Control	(C2) IPs Feed	
Blocklist.de	Block	IP	Basic HTTP	Public	Inbound +1	23,204	10/31/23, 02:28 PM	10/31/23, 02:28 PM	· 1			
CINS Army list	Block	IP	Basic HTTP	Public	Inbound +1	15,000	10/31/23, 02:28 PM	10/31/23, 02:28 PM				
CISA Alert List	Block	IP	CSV File Connector	Public	Inbound +1	399	10/31/23, 02:28 PM	10/31/23, 02:28 PM				
Cloud Attackers	Block	IP	CSV File Connector	Public	None	15,269	10/31/23, 02:42 PM	10/31/23, 02:42 PM	-			
Customer Manual List	Block	IP	Manual	Private	Inbound +1	2	10/31/23, 03:23 PM	10/31/23, 03:23 PM			Edit	
Cyjax	Block	IP	Cyjax	Public	None	49	10/31/23, 02:41 PM	10/30/23, 11:14 AM	-		Delete	
DHS Information	Block	IP	DHS Combined	Public	Inbound +1	0	10/31/23, 03:23 PM	06/18/23, 07:02 AM	DHS Information Sh	aring		
ET Block IPs	Block	IP	Basic HTTP	Public	Inbound +1	1,043	10/31/23,	10/31/23,				

• On the confirmation modal, select Delete

Delete List		
Are you sure you want to delete this List?		
Customer Manual List		
	Cancel	Delete

The list is now deleted.

NOTE: Lists that are tagged as "Public" Access cannot be deleted by end users.

Enforce

Enforce deploys and enforces data- in real time – at scale – across your entire network and blocks all known bad threat actors from ever entering your network. The Enforce menu options allow customers to view their Enforcers, and the pertinent data associated with each, install software builds, and configure their Networks and Ports.

Enforcers

The Enforcers tab displays all Enforcers that have been activated to your threatER account.

ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS
229 Build Numbe	er	11/1/2 Release D		Re	E olease Notes
Enforcers (1-3 total)					Save Subscriptions
All Support Statuses 🔹	All Bridge States	All Builds	▼ Reset		Filter Q
NAME 👙	SUBSCRIPTION	BRIDGE STATE	LD 🗇 LAST CONNEG	CTION 🖨	
APAC Edge	Threater	• Unknown 214	• 2 Updates Behind 05/30/23, 0	02:21 PM	Singapore
Europe HQ Edge	Threater	• Unknown 214	2 Updates Behind 05/30/23, 0	02:21 PM	London
North America HQ Edge	Threater	• Unknown 214	2 Updates Behind 05/30/23, 0	02:20 PM	New York
				PER PAGE: 20 👻	1-3 total < PREVIOUS 1 NEXT >

The following details display for each Enforcer:

- Enforcer Name This is generally provided during activation time, but can be changed as needed (see below for instructions). If no such name is available, a unique identifier is displayed.
- Subscription Enforce software subscription assigned to the Enforcer
 - See below more details on how to assign/unassign subscriptions
- Bridge State displays one of the following:
 - Normal
 - Hardware Bypass displays if the Enforcer is currently in hardware bypass mode

- Unknown displays for any Enforcer running legacy software, or if the Enforcer's current state is unknown
- Build Displays the Enforce software build the Enforcer is currently running. If the Enforcer is not on the latest build, the build number will display in red and a label will display indicating the number of builds the instance is behind
 - Scheduled displays the build schedule status. If there is no build status for the Enforcer, a "-" will display
- Last Connection displays the date and time the Enforcer last connected to the threatER portal. Normally, this should be within a few minutes of the present time.
- Location if a location has been provided by the user, it will display here. If no location has been
 provided, a "–" will display

To view additional details for an individual Enforcer click on the hyperlinked Enforcer name in the table. The additional data will display:

- Subscription Throughput refer to the Subscription Throughput section below for more details
- Admin IP of the Enforcer. This can be a great way for users to rediscover their administration IP if they've forgotten it and are in need of locally accessing Enforce, such as when working with our Customer Success team.
- Enforce Configuration Settings see Enforce Configuration section below for more details
- Networks being managed by the Enforcer

ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCF	RIPTIONS	REPORTS	
Enforcer Details Enforcer AW	S						
	ONNECTION SUPPORT E 23, 02:51 PM 12/31/202		BUILD NUMBER 229	SUBSCRIPTION THROUGHPU	T LOCATION AWS us-east-1	ADMIN IP 1.2.3.4	
Networks (1-2 of 2 total)							
All Configuration States	All Directions	✓ All Drop Actions	- Reset		Fil	Iter	С
NAME 🐡	DIRECTION	POLICY	DROP ACTION	IPS	PORTS		
NAME	DIRECTION	POLICY	DROP ACTION	IPS 10.0.1.0/24	PORTS All Protocols	DESCRIPTION	

Enforce Configuration

This section outlines the Enforce configurations that can be managed in the threatER Portal. To manage configurations in the portal, an Enforcer needs to be on Build 247 or later. Once an Enforcer is updated to Build 247, these configurations will be read-only in the Enforce UI.

Settings

The following Settings are available for configuration in the portal:

- Hostname
 - This field allows you to provide a unique label for the Enforcer.
- Timezone
 - This sets the timezone for the Enforcer. The best way to set the timezone is to type a city in the field. Options, based on your entry, will display in the drop-down and one can be selected.

ó

\$	SETTINGS	Hostname	Timezone
	SYSLOG	hostname	London 8 •
А	ACCESS		America/Toronto: Ontario London
		Login	Africa/Johannesburg: Eastern Cape East London
ŝ	BRIDGES	Maximum Login Attempts	Europe/London
C	NTP	5 30 timinutes	Europe/London: Inverclyde Greenock
$\mathbf{\Sigma}$	SMTP		Europe/London: Tyne and Wear Sunderland
	SMTP	Password	Europe/London: Southampton Southampton
÷**	SNMP	Minimum Duration 1 0 days 60 0 days	Europe/London: Bristol Bristol
			Europe/London: Bournemouth Bournemouth

- Login
 - You can set the maximum number of login attempts a user can make before being locked out.
 If locked out, you can set how long the user will be locked out for before they can attempt to
 login again. These settings apply to the Enforce UI and NOT to the portal.
- Session
 - You can set how long a user's active session can last and when their session will be timed out if they are inactive. These settings apply to the Enforce UI and NOT to the portal.
- Password
 - You can set how long a password is valid for, the required character length, and the minimum number of password groups the password must contain (i.e. special characters, uppercase, lowercase, etc.) These password settings apply to the Enforce UI and NOT to the portal.
- Banner

 Turning this setting on will enable a Terms of Service checkbox when a user attempts to login to the Enforce UI. If enabled, you can provide the text the user will see when accepting the Terms of Service, as well as what text will display if the user does not select the checkbox.

Accepted Text	Declined Text	· · · · · ·
I agree to the Terms and Conditions	I do not agree to the Terms a	nd Conditions





After making any changes on the Settings tab, be sure to click on the Save button in the top right corner.

Configu	ration		Save V			
\$	SETTINGS	Hostname	Timezone			
	SYSLOG	hostname	UTC -			
A	ACCESS	Login	Session			
e.	BRIDGES	Maximum Login Attempts Lockout Time	Maximum Duration Timeout			
0	NTP	5 30 © minutes	480 C minutes 60 C minutes			
	SMTP	Password				
+ ⁺ / ₀ +	SNMP	Minimum Duration 1 0 days 60 0 days	Minimum Length B 32 0			
			Minimum Character Groups			
		Banner				
		Cocceptor Text	Conclused Text I do not agree to the Terms and Conditions			

Syslog

Syslog exports are an industry-standard way of exporting data in a concise, timely manner. Our syslog export format is compliant to RFC-5424 and ensures seamless integration alongside any number of external tools like:

- Security information and event management (SIEM) tools, such as Splunk and IBM QRadar
- Data analytics tools like Gravwell
- Full open-source tools like syslog-ng

Our Syslog export is not designed with any particular SIEM tool in mind. We focus on the comprehensive data contained in our syslog exports, enabling you to parse our logs by any tool that can ingest RFC-compliant syslog exports.

To setup a syslog server:

- Click on the "New" button in the top right corner of the table
- Enter the following required fields:
 - Host
 - Port
- Provide a description (optional)
- Choose the Log Types to export
 - "All" is the default selection
- Select the desired Network
 - "All is the default selection
- Select the desired Verdict
 - "All is the default selection
- Select the desired Direction
 - "All is the default selection
- Choose the List Types(s), if desired
- Select the "Create" button in the bottom right corner

Configu	uration			Resat Save 🗸
¢	SETTINGS	Servers (1-0 of 0 total)	Filter Q New	Create Syslog Server
	SYSLOG	SERVER	LOG TYPES	Host Port 1.2.3.4 \$43
A	ACCESS	HOST PORT DESCRIPTION IF	SYSLOG AUDIT DNS DNS RESP	
ŀ	BRIDGES	No Syslog Serve	rs to Display	Description 0/128
G	NTP			Log Types
~	SMTP			☑ All ☑ IP ☑ Syslog ☑ Audit ☑ DNS ☑ DNS Response
* * *	SNMP			Network
				Or on List Type All All Allow Block Threat
				Cancel Croate

• Once all desired Syslog Servers have been added, select the Save button in to the top right corner

Config	uration				Reset Save 🗸
\$	SETTINGS	Servers (1-1 total)			Filter Q New
	SYSLOG	SERVER			LOG TYPES
	100500	HOST	PORT	DESCRIPTION	IP SYSLOG AUDIT DNS DNS RESP
A	ACCESS	➡ 1.2.3.4	443		
2	BRIDGES				PER PAGE: 20 V 1-1 total < PREVIOUS 1 NEXT >

Access

If your company has allowed Access rules to be managed in the threatER Portal (via a setting in the Enforce UI), the following protocols are available to add/edit:

- **HTTPS** This setting allows you to add internal networks that are allowed access to the admin interface of the threatER Enforcer.
- Ping The ping utility indicates if a particular internet address is accessible via the internet. This ping functionality can be abused by intruders, who may scan every internet address in a network, seeking out active targets. The Ping access setting allows you to block these intelligence-gathering scans by adding a list of trusted management networks. threatER Enforce will accept ping requests from these networks, and deny them from all others. By default, threatER Enforce will allow ping access from all IPv4 networks, as is indicated by the 0.0.0.0/0 address. After you allow access to your own local management networks, you can remove this "allow all" access by deleting it.

- **SNMP** The SNMP access setting allows you to add a list of trusted management networks. threatER Enforce will accept SNMP requests from these networks, and deny them from all others.
- SSH For any Enforcer in AWS, Azure, or Google Cloud, a default SSH access rule will be applied.

To add an Access rule:

- Click the "New" button in the top-right corner of the table
- Select the desired Protocol
- Enter the applicable Address
- Enter the applicable Maskbits
- Click the Create button

Confi	guration				Reset Save 🗸
\$	SETTINGS	Access Rules (1-2 total)	Filter Q	New	Create Access Entry
	SYSLOG	All Protocols (2) 🗸			Protocol Ping -
A	ACCESS	PROTOCOL 🔅 IP ADDRESS 🌍	MASKBITS		Address
e e	BRIDGES	HTTP 0.0.0.0		0	0.0.0.0
6	DIIDGLO	SSH 0.0.0.0		0	Maskbits
C	NTP	PER PAGE: 20 👻 1-2 to	otal < PREVIOUS 1 NE	ext >	0
\sim	SMTP				
	SNMP				Cancel Create

• Once all desired Access Rules have been added, select the Save button in to the top right corner

Config	uration	Reset Save ~		
	SETTINGS	Access Rules (1-3 total)		Filter Q New
	SYSLOG	All Protocols (3) 🗸		
A	ACCESS	PROTOCOL	IP ADDRESS 🐡	MASKBITS 🖨
e P	BRIDGES	+ Ping	0.0.0	0
6	DIIDGES	НТТР	0.0.0	0
C	NTP	SSH	0.0.0	0
\geq	SMTP		PER PAGE: 20 👻	1-3 total < PREVIOUS 1 NEXT >
4.20	SNMP			

To edit or delete an Access Rule, click on the ellipsis in the right hand column of the table and select the desired option.

6

Config	juration				Reset	Save 🗸	
:0:	SETTINGS	Access Rules (1-3 total)			Filter	Q New	
	SYSLOG	All Protocols (3) 👻					
A	ACCESS	PROTOCOL 🖨	IP ADDRESS		MA	SKBITS	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1
8.0		НТТР	0.0.0.0			0	
j.º	BRIDGES	SSH	0.0.0		Edit		
C	NTP	Ping	0.0.0		Delete		
\geq	SMTP			PER PAGE: 20 👻 1-3	total < PREVIOUS	1 NEXT >	
< <u>^</u>	SNMP						

Bridges

The Bridges tab displays the bandwidth or maximum rate of data transfer between the two bridge Ethernet ports. If Bypass is available, end users will be able to set the following modes:

- Bypass
- Startup
- Power-Off

If a Bypass Mode change is made, be sure to click the Save button in the top-right corner.

Config	uration							 Reset	Save	~
кўз	SETTINGS	brø 🔽	INSIDE enp7s0f0 SPEED 1 Gb/s full	Bypass	{• }	Current Mode	•			
	SYSLOG		OUTSIDE enp7s0f1			Startup Mode	•			
A	ACCESS	Q	SPEED 1 Gb/s full			Power-Off Mode				
şe	BRIDGES					bypass	•			
C	NTP									
\sim	SMTP									
4 ¹	SNMP									

NTP

The Network Time Protocol is a standard system for synchronizing the built-in clocks of network connected devices, to a very high degree of precision. Connecting threatER Enforce to the NTP network will ensure that the timestamps on its log files are accurate and coordinated with the computers in your organization.

threatER Enforce supports NTP version 3. Enter the IPv4 or IPv6 Internet address of your organization's NTP server, or if one isn't available, select a public server. Lists of time servers can be found at The NTP Public Services Project: http://support.ntp.org. NTPv3 has optional authentication. If required, click "Use Preshared Key" and enter the key information used by your selected time server.

For more accurate time synchronization, and as a guard against network outages, configure more than one timeserver.

Configuring the Time Zone and Date/Time settings can be done either manually or using an NTP server. Note that manually set times will be overwritten by the NTP Server settings.

To create an NTP Server:

- Click on the "New" button in the top-right corner of the table
- Enter the Host
- Click the "Create" button

Config	uration			Reset Save 🗸
:0:	SETTINGS	NTP Servers (1-1 total) @ Filter	Q New	Create Server
	SYSLOG	HOST		0.us.pool.ntp.org
A	ACCESS	time.google.com	0	
2	BRIDGES	PER PAGE: 20 💌 1-1 total < PREVIOUS	1 NEXT >	Cancel
0	NTP			

• Once all desired NTP Servers have been added, click the "Save" button in the top right corner.

Config	uration	Reset	`
\$	SETTINGS	NTP Servers (1-2 total) @	lew
	SYSLOG	ноят	
А	ACCESS	time.google.com	:
11	AUGLOS	♣ 0.us.pool.ntp.org	:
ľ	BRIDGES	PER PAGE: 20 👻 1-2 total < PREVIOUS 1 NEXT	
0	NTP		
Y	SMTP		

To edit or delete a NTP Server, click on the ellipsis in the right hand column of the table and select the desired option.

Configu	uration		Reset / Save
\$	SETTINGS	NTP Servers (1-2 total) @	Filter Q New
	SYSLOG	HOST	
А	ACCESS	time.google.com	
e.	BRIDGES	0.us.pool.ntp.org	Edit
°	NTP		PER PAGE: 20 - 1-2 total < P Delete
•	NIF		

SMTP

SMTP messages can be sent when an alarm is raised (e.g. an update fails, entering bypass mode or an account gets locked out).

To enable SMTP alerts:

- Set the Enabled toggle to the right
- Select the desired Protocol
- Enter the Host
- Enter the Port
- If authentication is required, provide the Username and Password
- Enter the "From Address"
- Enter the "To Address"

Once all fields have been provided, click the Save button in the top right corner.

Config	juration	Reset Save V
\$	SETTINGS	Enabled
	SYSLOG	Protocol SMTP Port 25
<i>I</i> A	ACCESS	Username Password &
L.	BRIDGES	From Address
C	NTP	To Address - user@threater.com
	SMTP	user e moduler.com
	SNMP	

SNMP

threatER Enforce supports the internet standard Simple Network Management Protocol (SNMP). Admins can remotely monitor Enforce by a network management system, such as IBM Tivoli Network Manager, CiscoWorks LAN Management Solution, and HP Network Node Manager.

Admins will need to set up SNMP access first before making SNMP configurations.

To configure SNMP, enter the following:

- Name
- Contact
- Port
- Location
- Description

threatER supports two versions of SNMP:

- Community-based SNMPv2c
- SNMPv3

Configu	uration								Reset	Save	
\$	SETTINGS	General									
	SYSLOG	Name SNMP Name				Contact SNMP Contact	t				
A	ACCESS	Port			\$	Location HQ					
2	BRIDGES	Description SNMP setup for HQ									
C	NTP										
Y	SMTP	v2 Users		ſ	Filter					Q	New
4 [†]	SNMP	COMMUNITY									
					No Items	to Display					
		v3 Users		ſ						Q	
		va Users			Filter					Q	New
			AUTHENTICATION				PRIVACY				
		USERNAME	ТҮРЕ	PASSPHR	ASE		TYPE	PASSPHRASE			<u> </u>
					No Items	to Display					,

Click the "New" button next to the desired version and provide the necessary details. Once complete, click the "Save" button in the top right corner.

Enforce Software

Customers can install the latest Enforce software build onto their Enforcers from the Enforcers tab.

The following software information is displayed on this tab:

- Build Number
 - Critical Update this will display if the build is critical in nature. Builds are flagged as critical if they include important security-related updates, critical bug fixes, or new features critical to the operation of the threatER platform. It is recommended to install critical updates as soon as possible.
- Release Date of the Build
- Release Notes selecting this will open a PDF of the Build Release Notes in a separate browser tab

ENFORCERS		NETWORKS	Ρ	ORTS	POLICIES	SUBSCRIPTIONS	REPORTS
	229 Build Numbe	r		11/1/2 Release D		Release Note	es
Enforcers (1-1 total) All Support Statuses	Ţ	All Bridge States	✓ All Bu	ilds	▼ Reset	Filter	Save Subscriptions
NAME 🖨		SUBSCRIPTION	BRIDGE STATE	BUILD 🖨	LAST CONNECTION		
HQ Enforcer		Enforce S	▼ Normal	219 9 Updates Behi	nd 11/09/23, 03:06 PM	West Region	* *
						PER PAGE: 20 - 1-1 total	< PREVIOUS 1 NEXT >

Users have the option to perform an immediate update, or to schedule an update.

Update Now

To immediately install the latest build on an Enforcer:

• In the row of the Enforcer, select Update Now from the ellipsis menu

All Support Statuses	 All Bridge States 	 All Builds 	▼ Reset	Filter	Q
NAME 🖨	SUBSCRIPTION	BRIDGE STATE 🖨 BUILD	LAST CONNECTION		
HQ Enforcer	Enforce S	Normal 219	9 Updates Behind 11/09/23, 03:06 PM	West Reg	idit 🚦
					Jpdate Now

• On the confirmation modal, select the Update button

Confirm Immediate Update	
Note the following: • Installing new software will force a reboot of the Enforcer. The instance will be offline	ne during the install.
This Enforcer will Update Immediately	
NAME	CURRENT BUILD
HQ Enforcer	219 9 Updates Behind
	Cancel Update

The table will display an "Update Pending" icon for the Enforcer until the build installation is complete. The "Update Pending" will automatically clear as soon as the associated Enforcer has begun the process of the update. Upon completion, which can take several minutes, the new build number will appear in the status.

Enforcers (1-1 total)					Save Subscriptions
All Support Statuses 🔹	All Bridge States	✓ All Builds	▼ Reset	Filter	Q
NAME 🕀	SUBSCRIPTION	BRIDGE STATE	Update Pending		
HQ Enforcer	● Enforce S ▼	Normal 219	9 9 Updates Behind 0 4 11/09/23, 03:23 PM	West Regior	n -

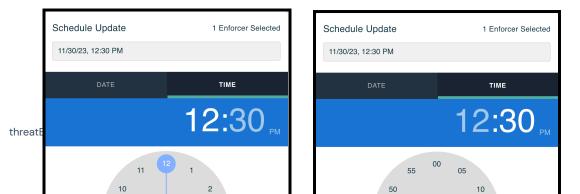
Schedule Update

Updates can be scheduled for one or more Enforcers. To schedule a build installation:

- Select the Enforcer(s) in the table
- Select the desired date in the calendar

Enf	Orcers (1-1 total)					Save Subsc		Schedu	le Upda	ite		1	Enforcer	Selected
All S	Support Statuses 🔹	All Bridge States	•	All Builds	▼ Reset	Filter	Q	11/30/23	8, 03:28 P	М				
	NAME © SUBSCRIPTION		GE STATE	BUILD 👙	LAST CONNECTI 11/09/23, 03	- 00			DATE				ТІМЕ	
	Enforcer Enforce S.	•	Normal	219 9 Updates Behind PER PAGE:	РМ	west Regio		²⁰²³ Thu,	Nov	30				
								<		No	vember 2	023		>
								S	М	т	W	т	F	S
											1	2	3	4
								5	6 13	7	8 15	9		11 18
								19		21			24	
								26		28	29	30		
												Ca	ncel S	chedule

• Select the Time tab and choose the desired time (both hours and minutes)



35

PLEASE NOTE: The time selected is in the user's local timezone, but saved in the backend in UTC. For example, if the user is located in New York City (EST) and selects 6:00PM, but the Enforcer is located in San Francisco (PST), the installation will begin at 6:00PM EST / 3:00PM PST.

- Select the Schedule button
- On the Confirm Scheduled Updates modal, select Schedule

Confirm Scheduled Update							
Note the following: Installing new software will force a reboot of the Enforcer. The instance will be offline during the install. If a new build becomes available between now and the Scheduled Date, the latest available build will be installed. 							
This Enforcer will Update 11/30/23, 12:30 PM							
NAME	CURRENT BUILD						
HQ Enforcer	219 9 Updates Behind						
	Cancel Schedule						

The table will reflect the schedules.

Cancel a Scheduled Update

To cancel a scheduled update:

• In the row of the Enforcer, select Cancel from the ellipsis menu

All Support Statuses All Bridge States All Builds Reset Filter Filter NAME SUBSCRIPTION BRIDGE STATE BUILD LAST CONNECTION LOCATION LOCATION LOCATION	Q
NAME SUBSCRIPTION BRIDGE STATE BUILD LAST CONNECTION LOCATION	
HQ Enforce S	Edit
PER PAGE: 20 🗸 1-1 total < PR	Update Now T >

• On the Confirm Cancel modal, select the Cancel button

6

Confirm Cancel	
Are you sure you want to cancel this Update scheduled for 11/3	0/23, 12:30 PM?
NAME	CURRENT BUILD
HQ Enforcer	229
Can	cel Cancel Update

The table will reflect the cancellation.

Revert to Previous Build

Users may have the ability to revert to the previous software build that was installed on an Enforcer, if both the previous and current versions, as a pair, are revertible. Reverts must be scheduled and can be done by completing the following steps:

• In the row of the Enforcer, select Schedule Revert to Build [#] from the ellipsis menu

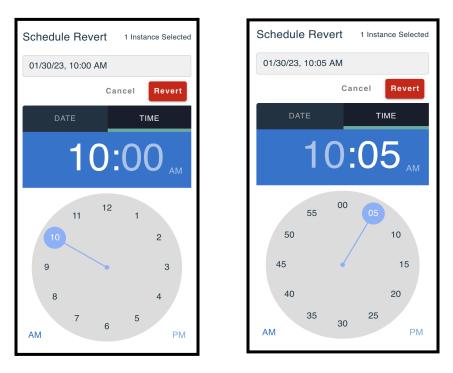
bs5.test	Threater	•	Normal	229	11/10/23, 10:36 AM	•	Edit	:
bs6.test	Threater	•	Normal	229	11/10/23, 10:36 AM		Update Now Schedule Revert to Build 228	
bs7.test	Threater	•	Normal	229	11/10/23, 10:36 AM			:

• Select a date from the calendar





• Select the Time tab and set the time (both hours and minutes)



PLEASE NOTE: The time selected is in the user's local timezone, but saved in the backend in UTC. For example, if the user is located in New York City (EST) and selects 6:00PM, but the Enforcer is located in San Francisco (PST), the installation will begin at 6:00PM EST / 3:00PM PST.

- Select the Revert button
- On the Confirm Scheduled Revert modal, select Revert

Confirm Scheduled Revert	4-
Note the following: • Installing new software will force a reboot of the Enforcer. The instance will be offline during the install. • This will install the previous software build your Enforcer was running on.	
This Enforcer will Revert to Build 228 11/30/23, 10:38 AM	
NAME	CURRENT BUILD
bs5.test	229
Cancel	Revert

The table will reflect the scheduled revert.

Manual Downloads

It is strongly recommended to utilize the automatic installation of Enforce software builds described in the above sections. Should a manual download of a build be required, please consult our <u>Customer Success team</u> for assistance. We do not recommend that you attempt Manual Downloads on your own without assistance. Use our automated mechanism as previously described unless instructed otherwise by our Customer Success team.

Subscription Management

To manage subscriptions from the Enforcers tab:

- Select (or remove) a subscription from the drop-down
- Make any additional necessary subscription updates to other Enforcers
- Select the Save Subscriptions button at the top of the table

ENFORCERS	NETWORKS	PORTS	\$	POLICIES	SUBSCRIPTIONS	REPORTS
22S Build Nur			11/1/23 Release Date		Release No	tes
Enforcers (1-1 total) All Support Statuses	All Bridge States	✓ All Builds	Ţ		Filter	Save Subscriptions
NAME 🖨	SUBSCRIPTION	BRIDGE STATE	BUILD 🖨	LAST CONNECTION		
HQ Enforcer	·	Normal	219 9 Updates Behind	11/09/23, 02:54 PM	West Region	:
	Enforce High Availability Subs Enforce Subscription Enforce Subscription	cription			PER PAGE: 20 v 1-1 total	< previous 1 Next >

• On the Save Changes modal, review the selected changes that were made and then select the Save button

Save Changes	
Are you sure you want to save?	
The following changes were made	
Removed (1 total)	^
Enforce Subscription Was removed from HQ Enforcer	
Added (1 total)	^
Enforce Subscription was added to HQ Enforcer	
Cancel Save Subscripti	ions

Subscription Status Indicators:

- Green subscription is actively supported
- Yellow support has lapsed; any Enforcee assigned a subscription in this state may not receive updated threat intelligence and as a result may be in an Allow–All state. You should contact our <u>Customer Success</u> team to review your subscription status.

Editing Enforcer Name and Location

To edit the Name and/or Location of an Enforcer to simplify your ability to identify your Enforcer according to your own network naming conventions:

- Find the Enforcer in the table and select the pencil icon in the far right column
- Enter the desired name and/or location
- Select Save

ENFORCERS	NETWORKS	PORTS		POLICIES	SUBSCRIPTIONS	REPORTS
22S Build Nun			11/1/23 Release Date			= se Notes
Enforcers (1-1 total) All Support Statuses	All Bridge States +	All Builds	▼ Reset Filt	Save Subscriptions ter Q	Edit Enforcer Name HQ Enforcer	
HQ Enforcer Enforce S.	BRIDGE STATE	210 9 Hodatas Bahind	LAST CONNECTION () 11/09/23, 02:57 PM	LOCATION 🐡	Vest Region	11 / 64
		PER PAGE: 20	v	PREVIOUS 1 NEXT >		Cancel Save

Subscription Throughput

The Subscription Throughout chart provides the past 30 days of an Enforcer's inbound and outbound throughput.

To access the Subscription Throughput chart click on an individual Enforcer and then select the Subscription Throughput bar.

ENFORCE	rs r	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS
Enforcer Details						
SUPPORTED	LAST CONNECTION 11/09/23, 02:59	PM Normal	BUILD NUMBER 219	SUBSCRIPTIO	0% West Region	ADMIN IP 10.0.36

The following throughput details will display at the top:

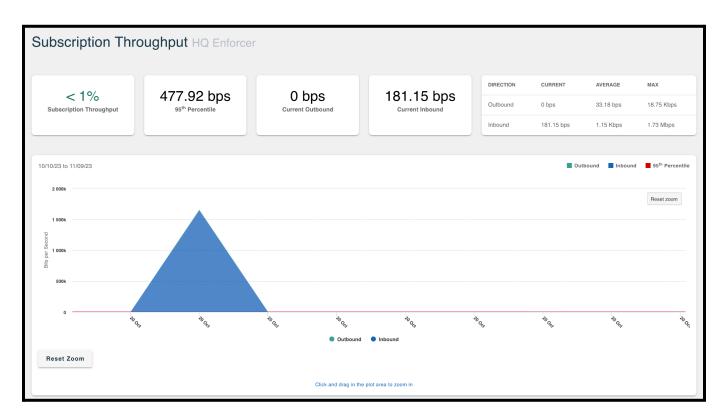
- % Subscription Throughput utilized for the past 30 days
- 95th Percentile for the past 30 days, via industry standard 95/5 measurements
- Current Outbound throughput (in bits)

• Current Inbound throughput (in bits)

The table in the top right corner will display the following inbound and outbound data:

- Current throughput (in bits per second)
- Average throughput (in bits per second)
- Maximum throughput (in bits per second)

The chart displays a graphical representation of the inbound and outbound throughput and the 95th percentile for the past 30 days. You can click and drag within the plot area to zoom in to a specific date/time.



Networks

Enforce inspects Network traffic to determine which packets to block and which to allow. Policies attached to Networks determine the internet services allowed into your network, as well as those services your local users can access outside the network.

threateg

One or more network rules comprise a configured Network in threatER, and each network is identified as a device, asset, or subnet on your network. If the Enforcer receives traffic for the configured IP, then it will allow traffic according to the policy associated to the Network. Each Network configuration includes a protocol and port, or range of ports, so that you may restrict specific policy activity to as granular a level as required.

NOTE: An Enforcer must have an Enforce build greater than 180 installed to fully take advantage of this feature within the portal. As such, we strongly urge customers to update to the latest software to be able to use these powerful centralized control features. Customers who have not yet updated are not able to control these features centrally, and instead must leverage the legacy Enforce UI elements.

Creating Networks

To create a Network:

- Navigate to Enforce in the left-hand navigation menu
- Select the Networks tab
- Select the "Create" button in the top-right corner

= threater									<u> २</u>
E Collect	ENFORCE	-00	NETWORKS	PORTS		POLICIES	SUBSCRIPTIONS	REPOR	
Enforce	ENFORCE	.45	NETWORKS	PORTS		POLICIES	SUBSCRIPTIONS	REPOR	15
🕁 Marketplace	Networks (1-1 to	tal)							Create
4 Messages	All Configuration S	tates -	All Directions	✓ All Enforcers	•	All Drop Actions	← Reset	Filter	Q
Administration	NAME 😄	DIRECTION	POLICY	ENFORCER 👙	DROP ACTION	IPS	PORTS		
{} API Docs	All traffic	Inbound Outbound	Inbound Outbound	HQ Enforcer	Discard TCP Reset	0.0.0/0	All Protocols		:
							PER PAGE: 20 👻	1-1 total < PREVIOUS	NEXT >

Network Details

Provide the following (* indicates required field):

- *Name (unique name required)
- Enter an optional description
- Enforcers
 - Select the desired Enforcer(s) from the drop-down
 - NOTE: Enforcers on Enforce Build 154 or prior build will not display in this drop-down.
- *Direction

- Inbound determines the kind of internet traffic allowed into your network. Each inbound rule shows a particular computer and service that will be visible to the internet.
- Outbound determines how your local computers can access the internet. Each outbound rule shows which particular outside internet service a computer can access.

Once all required fields are complete, select the Next button to proceed to the next step.

Create Network			
		ks created in Threater determine the internet services allowed k in Threater, and each is identified as a device, asset, or subr	
NETWORK DETAILS	(3) INBOUND	OUTBOUND	IPS
Network Details			
Name All traffic			
Description			11 / 64
- Enforcers			0 / 128
HQ Enforcer			•
Both			•
			Next

Inbound/Outbound

Provide the following for the Direction(s) selected in the previous step (* indicates required field):

- *Policy
- *Drop Action
 - Discard drops the packet and does not send any response (silently discards it). This is useful especially for inbound attempts, so that malicious attackers are not necessarily able to determine your presence
 - ICMP Unreachable drops the packet and sends an ICMP unreachable packet to the sender.
 This is generally recommended only for use with outbound policies.
 - TCP Reset drops the packet and sends a TCP Reset packet back to the sender.
 Recommended only if the firewall doesn't properly allow ICMP Unreachable messages.
 Additionally, this is generally recommended only for use with outbound policies.

Select Next to proceed to the next step.

Create Network		at the second se
Enforce inspects Network traffic to determine which packets to block and which to allow. Netwo your local users can access outside the network. One or more network rules comprise a Networ		
NETWORK DETAILS INBOUND	OUTBOUND	(d) IPS
Inbound Select or Greate a Policy Inbound		• New Policy
Drop Action Discard Only		•
Previous		Next

If "Both" was chosen as the Direction on the Details step, the next step will be the same as above, but for the Outbound direction.

Create Network			
		orks created in Threater determine the internet services allo rk in Threater, and each is identified as a device, asset, or	
NETWORK DETAILS	INBOUND	OUTBOUND	() IPS
Outbound Select or Create a Policy Outbound Drop Action ICMP Unreachable			• New Policy
Previous			Next

Create New Policy During Network Creation

If a policy does not exist that you want to apply your Network to, you have the option to create a new policy within the Network wizard. To do so, select the "New Policy" button on the Inbound and/or Outbound step and then follow the steps to create a policy, outlined above in the Policies section of this document.

IPs

To add IPs to your Network, provide the following (* indicates required field):

- *IP address
- *Maskbits
- Description
- *Port
 - All Protocols is the default selection
 - To choose a Port you have previously configured, click on the drop-down and select the desired option
 - To create a new Port:
 - Click on the Create button

Add IP		
0.0.0.0		
C Maskbits		
O		\$
Description		
Select or Create a Port		0 / 128
All Protocols		Create
	Cancel	Add

- Provide the following (* indicates required field):
 - *Name
 - Description
 - *Protocol

Ó

- "All: 256" is the default selection, but another protocol can be selected from the drop-down
 - You will be required to provide a Port or Port Range for some protocols, such as TCP and UDP

Ó

- Click on the +Add button to add the Protocol
- Add any additional Protocols, as necessary

Create Port			
Name Customer Port			
			13 / 64
Description			
			0 / 128
PROTOCOL		PORT(S)	
	No Se	rvices. Add some below	
Protocol		C Ports	-
TCP: 6	*	50-2489	⊕Add
The TCP Protocol us	es Ports. El	nter them above. eg: 22 or 42	58
		Cancel	Create

- Click the Create button to return to the Add IP Panel
- Select the Add button to add the IP to the Network

threateg

Create Network				
	affic to determine which packets to block and which to allow. Networks created outside the network. One or more network rules comprise a Network in Threate			
NETWORK DETAILS		OUTBOUND		() IPS
Set up your IPs		Remove	Add IP	
IP	MASKBITS PORT DESCRIPTION		IP 0.0.0.0	
	Add IPs to this Network		Maskbits	
	To add an IP to this Network, enter the IP address, maskbits, Port, and click Add.		Description	
			Select or Create a Port	0 / 128
				Cancel Add

• Follow the steps above to add additional IPs

Once all IPs are added, select the Create Network button to create the Network.

NETWORK DETAILS	INBO		OUTBOUND	,	d IPS
Set up your IPs			Remove	Add IP	
IP IP	MASKBITS PORT	DESCRIPTION		IP	
0.0.0	- Customer F	Port -			
				Maskbits	
				Description	
				Select or Create a Port	07
				All Protocols	- Crea
					Cancel Ac
Previous					Create Networ

Editing a Network

To Edit a Network:

• Find the Network in the table and from the ellipsis menu, select Edit

All Configuration	States - A	II Directions	✓ All Enforcers	•	All Drop Actions	- Reset	Filter	Q
NAME 🔶	DIRECTION	POLICY	ENFORCER 🐡	DROP ACTION	IPS	PORTS		
All traffic	Inbound Outbound	Inbound Outbound	HQ Enforcer	Discard TCP Reset	0.0.0/0	All Protocols	Edit Delete	:

- Edit Network Details -
 - This Is the default view when editing a Network. Make any necessary edits and then select another step that requires updates.
 - If edits are only needed on this step, select the Save button in the top right corner

Edit Network All traffic			Cancel Save
	etermine which packets to block and which to allow. Network the network. One or more network rules comprise a Network		
NETWORK DETAILS	INBOUND	OUTBOUND	IPS
Network Details			
All traffic			
Description			11 / 64
C Enforcers			0 / 128
HQ Enforcer			•
Directions			
Bour			•

- Edit Direction(s) (Inbound/Outbound) -
 - Select this step(s) to update the Policy and/or Drop Action
 - If no other Network edits are desired, select the Save button in the top right corner
 - If additional edits are needed, select the applicable step

threateg

Edit Network All traffic	Cancel Save
Enforce inspects Network traffic to determine which packets to block and which to allow. Networks created in Threater determine the internet service your local users can access outside the network. One or more network rules comprise a Network in Threater, and each is identified as a device, ass	
NETWORK DETAILS OUTBOUND	PS IPS
Inbound	
C Select or Create a Policy	
Inbound	New Policy
C Drop Action	
Discard Only	•

o IPs -

- Select this step to add or remove IPs
- Refer to the IPs section above for guidance
- If no other Network edits are desired, select the Save button in the top right corner

Edit	Network All tra	affic					Cancel Save
						the internet services allowed on your net d as a device, asset, or subnet on your n	
NETV	/ORK DETAILS		INBOUND		OUTBOUN	ND	IPS
Set u	ıp your IPs				Remove	Add IP	
	IP	MASKBITS	PORT	DESCRIPTION		IP	
	0.0.0.0		All Protocols			Maskbits	0
						WIASKUIS	~
						Description	
						Select or Greate a Port All Protocols	0 / 128
							Cancel Add

Deleting a Network

To delete a Network:

- Find the Network in the table
- Find the List in the table and from the the ellipsis menu, select Delete

Networks (1-1 to	stal)							Create
All Configuration S	itates -	All Directions	✓ All Enforcers	•	All Drop Actions	- Reset	Filter	Q
NAME ≑	DIRECTION	POLICY	ENFORCER 🖨	DROP ACTION	IPS	PORTS		
All traffic	Inbound Outbound	Inbound	HQ Enforcer	Discard TCP Reset	0.0.0/0	All Protocols	- Edit.	. :

• On the confirmation modal, select Delete

Delete Network	
Are you sure you want to delete this Network?	
All traffic	
Cancel	Delete

The Network is now deleted.

Ports

Ports define the protocols for a given Port and can be used across multiple Networks for allowing or blocking defined Ports.

Adding Ports

To add a Port:

- Navigate to Enforce in the left-hand navigation menu
- Select the Ports tab
- Click on the "Create" button in the top right corner of the table

= threater						<u>२</u>
E Collect	ENFORCEDO	NETWORKS	DODTO	ROUGIES		REPORTS
Enforce	ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS
🔄 Marketplace	Ports (1-2 total)				· · · · · · · · · · · · · · · · · · ·	Create
4 Messages	All Protocols				Filter	Q
Administration	NAME 🖨	PROTOCOLS	S ≑	NETWORKS 🖨	DESCRIPTION	
{} API Docs	Customer Port	TCP: 50-248	189			:
	Customer Protected Port	ICMP TCP: 50-248	489		Adding ICMP Protocol	:
					PER PAGE: 20 👻 1-2 total	< PREVIOUS 1 NEXT >

- Provide the following (* indicates required field):
 - *Name
 - Description (optional)
 - *Protocol
 - "All: 256" is the default selection, but another protocol can be selected from the drop-down
 - You will be required to provide a Port or Port Range for some protocols, such as TCP and UDP
 - Click on the +Add button to add the Protocol to the Port

Create Port			
Additional Port			
			15 / 64
Description			
			0 / 128
PROTOCOL		PORT(S)	
	No Ser	vices. Add some below	
		- Ports	_
Protocol UDP: 17	•	50-2489	Add
The UDP Protocol u	ses Ports. Er	iter them above. eq: 22 or 42 - 1	138
			_
		Cance	Create

- Add any additional Protocols to the Port, as necessary
- Click the Create button to create the Port

threateg

Editing Ports

To edit a Port:

• Find the Port in the table and from the the ellipsis menu, select Edit

		Filter		Create
		Filter		
		Filter		Q
PROTOCOLS 🍦	NETWORKS	DESCRIPTION		
UDP: 50-2489				
TCP: 50 2480			Edit	
ICMP TCP: 50-2489	•	Adding ICMP Protocol	Delete	
		PER PAGE: 20 - 1-3 total	< PREVIOUS 1	NEXT)
	UDP: 50-2489 TCP: 50-2489 ICMP	UDP: 50-2489 - TCP: 50-2489 - ICMP -	UDP: 50-2489 - - TCP: 50-2489 - - ICMP TCP: 50-2489 - -	UDP: 50-2489

• Make the necessary changes and click the Save button

Ports (1-3 total) All Protocols	•		Filter	Create	Edit Port Name Customer Port		13 / 64
NAME 😄	PROTOCOLS 🚖	NETWORKS 🚖			Description		
Additional Port	UDP: 50-2489	-	-				
Customer Port	TCP: 50-2489	-		:	PROTOCOL	PORT(S)	0 / 128
Customer Protected Port	ICMP TCP: 50-2489	-	Adding ICMP Protocol	:	TCP: 6	50-2489	Ō
		PER PA	GE: 20 👻 1-3 total < PREVIOUS	1 NEXT >	Protocol All: 256		▼ ⊕Add
						Can	save

Deleting Ports

To delete a Port:

• Find the Port in the table and from the the ellipsis menu, select Delete

Ports (1-3 total)				Crea	ite
All Protocols				Filter	9
NAME 🖨	PROTOCOLS 🌐	NETWORKS 🐡	DESCRIPTION		
Additional Port	UDP: 50-2489		. 7		:
Customer Port	TCP: 50-2489		· [.		:
Customer Protected Port	ICMP TCP: 50-2489	-	Adding ICMP Protocol	Edit	:
			PER PAGE: 20 👻	1-3 total < PR	r >

• On the confirmation modal, select the Delete button

Delete Port	
Are you sure you want to delete this Port?	
Customer Protected Port	
Cancel	Delete

The Port is now deleted.

Policies

Policies allow users to determine what is or is not allowed through specific networks or network segments. As there are no limits to the number of policies that can be created, users can create as many or as few policies as they need to protect each of their networks as they deem necessary.

Create a Policy

To create a Policy:

- Navigate to Enforce in the left-hand navigation menu
- Select the Policies tab
- Select the Create button the top-right corner of the table

= threater						<u> २</u> ७ ७
E Collect	ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	
Enforce	ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS
🔂 Marketplace	Policies (1-2 total)				••••••••••••••••••••••••••••••••••••••	Create
4 Messages	All Networks -				Filter	٩
Administration	NAME 🗇	NETWORK 🖨 DIR	ECTION	DESCRIPTION 👙		
{} API Docs	Inbound	All traffic	Inbound	all inbound traffic		:
	Outbound	All traffic	Outbound	all outbound traffic		:
					PER PAGE: 20 👻 1-2 total	< PREVIOUS 1 NEXT >

Policy Details

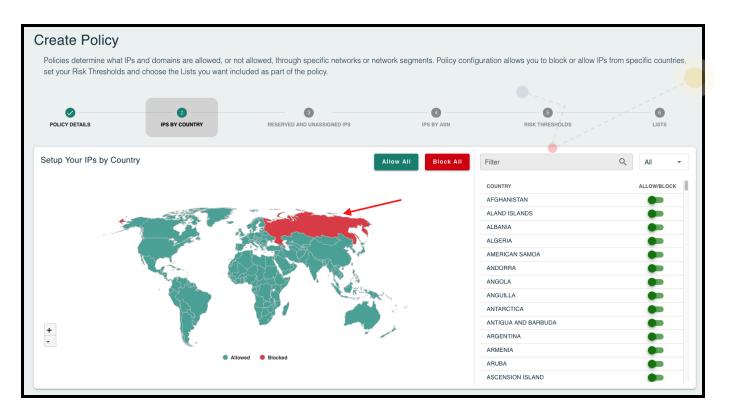
Enter a name (required) and optional description for the Policy, then select the Next button.

	IPs and domains are allowed, or r and choose the Lists you want in	not allowed, through specific networks or netw ncluded as part of the policy.	work segments. Policy configur	ation allows you to block or allow IPs f	from specific countries,
POLICY DETAILS	IPS BY COUNTRY	RESERVED AND UNASSIGNED IPS	IPS BY ASN	RISK THRESHOLDS	6 LISTS
Set up your Policy deta Name General Policy	ails				8
Description					14/64
					0/128

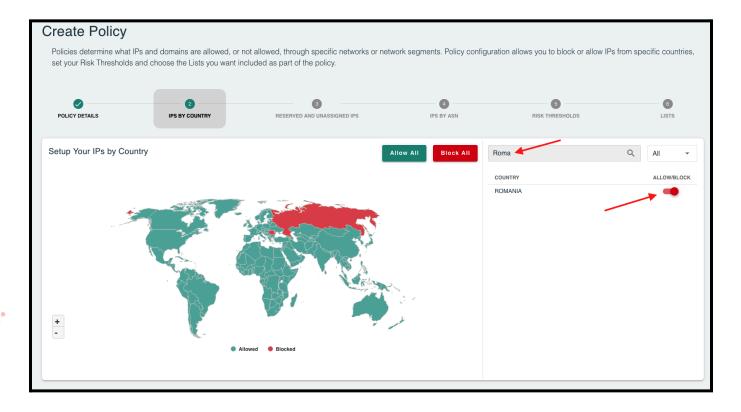
IPs by Country

By default, IPs from all countries are allowed. Traffic can be blocked from specific countries one of two ways:

• Option 1 - Click on a country in the map to change it to the block setting (country will now be red)



• Option 2 - Search for the country in the Filter box and then move the toggle to the Block state



- Alternatively, you could select 'Block All' and start selectively allowing individual countries. This can be a great way to geo-block most of the world except the areas in which you do business.
- Once all IPs by Country settings are complete, select the Next button

Reserved and Unassigned IPs

Reserved and Unassigned IPs are allowed, by default, to help prevent internal IPs from being blocked. To block either, select the Block button(s) and then select Next.

	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS
Policies determine what IPs and o	domains are allowed, or not allow				
	domains are allowed, or not allow				
set your Risk Thresholds and cho	pose the Lists you want included a		work segments. Policy configur	ration allows you to block or allow IPs	from specific countries,
POLICY DETAILS	IPS BY COUNTRY	3 RESERVED AND UNASSIGNED IPS	IPS BY ASN	C RISK THRESHOLDS	6 LISTS
et up your Reserved and Una	assigned IP Settings				
eserved IPs					Allow Block
nassigned IPs					Allow Block
Previous					Next

IPS by ASN

Traffic can be allowed or blocked from a single autonomous system number (ASN). This can be a useful feature when you are relying on large-scale geo-blocking, but find the need to allow one or more ASNs in a given country while maintaining blocks on all other activity associated with that country. Similarly, it can be a great way to quickly block all activity to and from ASNs that have been compromised or are being heavily used by malicious actors.

To add an ASN to your policy:

- In the right-hand panel, search by ASN Name or ASN Number
- Click on the verdict you want to apply to that ASN (Allow or Block) to add it to the left-hand panel

	and choose the Lists you want in	not allowed, through specific networks or networks or networks or networks or networks or networks or networks and the policy.	с ,			
_	_			•		11
POLICY DETAILS	IPS BY COUNTRY	RESERVED AND UNASSIGNED IPS	4 IPS BY ASN	6 RISK THRESHOLDS		LISTS
All Verdicts	•	Filter	Q	dropbox		(
AME		ASN	VERDICT	PER PAGE: 20 👻	PREVIOUS 1 N	EXT >
ropbox		1000019851	Allow Block	NAME	ASN	VERDICT
				Dropbox	1000019851	Allow BI
				Dropbox Inc	393874	Allow BI
				Dropbox Inc.	62190	Allow BI
				Dropbox Ireland Limited	1000021244	Allow BI
				Dropbox, Inc.	19679	Allow BI
				Dropbox, Inc.	54372	Allow BI

• Repeat for any other ASNs you want to add

To remove an ASN click on the trash icon in the row of the ASN.

POLICY DETAILS	IPS BY COUNTRY	RESERVED AND UNASSIGNED IPS	IPS BY ASN	RISK THRESHOLDS	6 LISTS
All Verdicts	•	Filter	Q	microsoft corp	Q
NAME		ASN	VERDICT	PER PAGE: 20 👻 < PREVIOUS	NEXT >
Dropbox		1000019851	Allow Block		
Digital Ocean		1000001621		NAME	SN VERDICT
Microsoft Corp		1000016051	Allow Block	Microsoft Corp 45	Allow Block
				Microsoft Corp 1000016	051 Allow Block

Click the Next button when all desired IPs by ASNs verdicts are applied.

Risk Thresholds

There are <u>many threat categories</u> that can be enabled. All IPs included in the threat lists are placed in one or more of these categories. Each IP in the threat intelligence also has an associated score that can range from 1 to 100, with a higher score representing a higher confidence of it being malicious, as rated by our feed

partners. Enabling categories and setting Risk Thresholds allows you to control how strong of a policy you want to apply. Since the Risk Threshold setting indicates confidence in malicious activity, the lower this is set, more traffic will be blocked.

As an example, if the Command and Control category is enabled with a threshold of 90, any IP identified as a Command and Control with a score of 90 or above will be blocked. If the Command and Control category was not enabled, the connection would be allowed through by the threat list, but could still be blocked by other categories (since an IP or domain can appear in multiple categories), Block lists, IPs by Country policy, and so on.

POLICY DETAILS	IPS BY COUNTRY	RESERVED AND UNASSIGNED IPS	IPS BY ASN	3 RISK THRESHOLDS	6 LISTS
Set up your Risk Thres	hold Settings				
NAME			Set All 🗘		
Advanced Persistent Th	nreat		75 😂		
Botnet			75		
Brute Force Password			Not Set 🗘		
Command and Control			90 🗘		
Compromised			Not Set 😂		
DDOS			90 0		
Drop Site			Not Set 🗘		
Endpoint Exploits			90 0 😒		
Fraudulent Activity			Not Set 😂		
Illegal Activity			Not Set		
Online Gaming			Not Set		

To enable a category, select the checkbox to the left of the desired category. To enable all categories, select the checkbox at the top of the column. As a matter of best-practice, we strongly recommend enabling all categories.

To set a Risk Threshold for a category, enter a value between 1 and 100 in the text field to the right of the category. To apply the same Risk Threshold to all categories, enter your value in the text field at the top of the column.

POLICY DETAIL	S IPS BY COUNTRY	RESERVED AND UNASSIGNED IPS	IPS BY ASN	5 RISK THRESHOLDS	G LISTS
Set up your	Risk Threshold Settings				
NAME			90 🗢		1
Advanc	ed Persistent Threat		90 0	•	
Botnet			90 0		
Brute F	orce Password		90 0		
Comma	and and Control		90 0		
Compro	omised		90 0		
DDOS			90 0		
Drop Si	te		90 0		
Endpoir	nt Exploits		90 0		
Fraudul	lent Activity		90 0		
Illegal A	Activity		90 0		
Online	Gaming		90 🗘		

Once all settings have been applied, select the Next button.

Best Practice Recommendation for Risk Thresholds:

We recommend a value of 80 for customers who want to be aggressive (more will be blocked), and 90 for those who want to be more conservative (less will be blocked). If you need to block more IPs in a certain category, lower the score in that category. If you want to block fewer IPs in a certain category, raise the score in that category.

For example, if you're hearing that many legitimate sites or services are being blocked, and upon correlating with your logs find that they are being marked as spam with a score of 90–94, you can raise the threshold for the Spam category to 95. Now, you will see fewer unexpected blocks based on Spam.

On the other hand, if you are checking your logs and seeing many unidentifiable Endpoint Exploits are getting through with a score of 85–89, you can lower the score to 85. Now, you will see more blocks based on Endpoint Exploits.

Lists

Users can enable Allow, Block, and Threat Lists per policy, which specifies the IPs and/or domains that should be allowed or blocked on the policy. **Allowed and Blocked Lists do not influence traffic until enabled on a Policy.**

To include a List as part of your policy, search for the List(s) (you can utilize the Filter at the top of each panel) and then select the checkbox next to each desired List.

POL	CY DETAILS	IPS BY COUNTRY	RESER	RVED AND UNAS	SIGNED IPS IPS BY ASN			RISK THRESHOLDS	6 LISTS
Allow	Lists	5 of 16 lists selected	Block	k Lists	All 21 lists sele	ected	Threat Lis	ots	All 1 lists selected
	Filter	Q		Filter		Q	Filte	r	Q
	IP	Akamai		Domain	Bambenek ML-Malware		IP	Webroot	
~	IP	Amazon Cloudfront		Domain	Bambenek ML-Phishing				
	IP	Cisco Webex		Domain	Bitdefender APT-Domains				
	IP	Cloudflare CDN	~	IP	Bitdefender C2-IPs				
\checkmark	IP	Docusign	~	Domain	Bitdefender Malicious-domains				
~	Domain	DocuSign	\checkmark	Domain	Bitdefender Phishing-domains				
	IP	Fastly	\checkmark	IP	Blocklist.de				
	IP	Github		IP	CINS Army list				
	IP	Google		IP	CISA Alert List				
	IP	Mailchimp		IP	Cloud Attackers				
	IP	Pingdom		Domain	Customer Manual Domain List				
	IP	Survey Monkey		IP	Customer Manual List				
_		~ ···	_	-	<u>.</u>				

Once all desired Lists have been selected, select the "Create Policy" button. Your policy is now created.

Best Practice Recommendation for Lists:

We recommend the following:

- Allow Lists Enable only the lists/services you want allowed for the specific policy. Generally these
 would be services that your business is reliant on. We strongly recommend that you always enable
 the threatER Curated DNS and threatER SaaS lists, especially for outbound policies, to ensure
 that your environment never loses connectivity to critical threatER resources.
- Block Lists Enable all Block Lists, except for Zoom, which can be enabled at your discretion.

Creating an Allow All Policy

Allow All policies can be used as a "break glass" policy in cases where a business critical site or service must be accessed, but is being blocked. By using an Allow All policy, all traffic is allowed through the Enforcer and continues to be logged for review. We recommend using this policy instead of putting the device into <u>bypass</u> <u>mode</u> if you don't know whether or not the threatER platform is blocking this traffic, so that logging is maintained. In bypass mode, no traffic is logged.

To create an Allow All policy, apply the following configurations on each step:

- IP by Country: Allow All
- Reserved and Unassigned IPs: Allow both
- Risk Thresholds: Disable (uncheck) all categories
- Lists: Disable (uncheck) all Block & Threat lists

Edit a Policy

To edit configurations of an existing policy:

- Find the Policy that needs configuration edits in the table
- From the ellipsis menu in the row of the policy, select Edit

ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS	5
Policies (1-2 total)					1	Create
All Networks -				Filt	er	Q
NAME 😄			DESCRIPTION			
Inbound	All traffic Inhound		all inhound traffic		Edit	:
Outbound	All traffic Outbound)	all outbound traffic		Delete	:
				PER PAGE: 20 👻 1-2 to	otal < PREVIOUS 1	NEXT >

- Click on the Policy step that needs adjustments and make the necessary edits
- Click on any other steps that needs adjustments and make those edits

After you have completed all desired edits, click Save to enact all policy edits. Your changes will temporarily save step to step within the wizard, but will be lost unless you click the Save button.

Edit Policy Inbound Policies determine what IPs and domains are allowed, or not allowed, through specific networks or network segments. Policy configuration allows you to block or allow IPs from specific count set your Risk Thresholds and choose the Lists you want included as part of the policy.				
	Cancel Save		y Inbound	Edit Policy
POLICY DETAILS IPS BY COUNTRY RESERVED AND UNASSIGNED IPS IPS BY ASN RISK THRESHOLDS LISTS	SIGNED IPS IPS BY ASN RISK THRESHOLDS LISTS	RESERVED AND UNASSIGNED IPS	IPS BY COUNTRY	POLICY DETAILS

Delete a Policy

A Policy can only be deleted if there are no Networks utilizing that policy.

To delete a Policy with no Networks assigned to it:

- Find the Policy in the table
- From the ellipsis menu in the row of the policy, select Delete

Policies (1-3 total)				Create
All Networks -			Filter	Q
NAME 😄	NETWORK 🗇 DIRECTION	DESCRIPTION		
Inbound	All traffic Inbound	all inbound traffic		:
New Policy			Edit	:
Outbound	All traffic Outbound	all outbound traffic	Delete	:
		PER PAGE: 20 👻	1-3 total < PREVIOUS 1	NEXT >

• On the confirmation modal, select Delete

Delete Policy	
Are you sure you want to delete this Policy?	
New Policy	
Cancel	Delete

To delete a policy that is being utilized by a Network, please refer to the steps to remove a policy from a Network first.

Subscriptions

Enforcers log traffic, filter traffic, and receive updated threat intelligence with a supported subscription. Without a valid attached subscription, the Enforce software will blindly forward traffic in both directions with no filtering action and no logging. The Subscriptions tab can be used to assign subscriptions accordingly.

The following will display on this tab:

- Enforcers
 - Displayed in the left-hand column
 - Enforcer Statuses
 - Green Enforcer is assigned an active subscription
 - Yellow Enforcer is assigned a subscription that is no longer under active support; any Enforcer assigned a subscription in this state may not receive updated threat intelligence and as a result may be in an Allow–All state. You should contact our <u>Customer Success</u> team to review your subscription status.
 - Red Enforcer does not have a subscription assigned to it; the Enforcer will not receive updated threat intelligence and will be in an Allow-All state
- Subscriptions
 - Displays the subscription assigned to the Enforcer

= threater							0 9
E Collect	ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS	
Enforce							
Aarketplace	Enforcers (1-1 total)						Save
යු ³ Messages	All Support Statuses 👻				Fil	ter	Q
Administration	NAME 😄					SUBSCRIPTIONS	
{} API Docs	HQ Enforcer					Enforce Subscri	•
					PER PAGE: 20 👻 1-1	total < PREVIOUS 1 NE	EXT >

To assign a subscription to an Enforcer:

• Select the subscription from the drop-down

ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS
Enforcers (1-1 total) All Support Statuses				Filter	Save
NAME 😄				SUB	SCRIPTIONS
HQ Enforcer				PER PAGE: 20 1-1 ● E	Enforce Subscri 😢 🔺 nforce High Availability Subscription nforce Subscription nforce Subscription

• Select the Save button

ENFORCERS		POLICIES	SUBSCRIPTIONS	REPORTS
Enforcers (1-1 total)				
All Support Statuses			Filt	er Q
NAME 🗇				SUBSCRIPTIONS
HQ Enforcer				Enforce Subscri
			PER PAGE: 20 💌 1-1 t	tal < previous 1 NEXT >

• On the Save Changes modal, review the selected changes that were made and then select the Save button

Save Changes		
Are you sure you want to save?		
The following changes were made		
Removed (1 total)		^
Enforce Subscription was removed from HQ Enforcer		
Added (1 total)		^
Enforce Subscription was added to HO Enforcer		
	Cancel	Save

threateg

Unexpected Blocks

PREREQUISITE: To access and utilize this feature, all Enforcers on your account need to be updated to BUILD 240 or later.

threatER's Unexpected Blocks feature allows you to retrieve outbound Port 80 and 443 traffic logs that your Enforcer(s) have blocked. These logs enable portal users to make an informed decision on whether to allow those IPs.

To perform an analysis:

- Navigate to Enforce in the left-hand navigation menu
- Select the Unexpected Blocks tab
 - This tab will NOT appear until all Enforcers tied to your portal account have been updated to at least Build 240
- Select a Date Range and the Enforcers you want to query logs on
 - Default selections are the last 3 hours and All Enforcers
- Click Submit

= threater			9 Ø
E Collect			
Enforce	ENFORCERS NETWORKS PORTS POLICIES SUBSCRIPTIONS UNEXPECTED BLOCKS RE	PORTS	
合 Marketplace	Do you have a connection to a website being blocked unexpectedly? Threater's Unexpected Blocks feature allows you to retrieve logs from your Enforcer that include the pertinent data to identify the problematic IP and make an informed decision on whether to allow it. For more information on Unexpected Blocks, please refer to our <u>support site</u> and <u>blog post</u>	1	×
A Messages	 procentation in and make an informed decision on whether to anow it. To more information on onexposed blocks, prease relie to our <u>asked tate</u> and <u>taxy toos</u> 		
Administration	Initiate Log Analysis		
{} API Docs	C Last 3 Hours All Enforcers Reset	Subm	iit

Please note: The length of time associated with available results varies based on the parameters selected, your network activity/connection, and the resources (such as system RAM) of your Enforcers. The progress of your analysis is available on the Unexpected Blocks tab. You can navigate away and perform other functions within the application while your analysis is processing, but if you logout or close your browser your results will not complete.

Once your submitted query is complete, the log entries will display on the Unexpected Blocks tab. To view additional data in each entry, expand the row via the disclosure triangle in the far left column. The additional

information can be very useful when determining whether or not an IP that is currently being blocked should be allowed.

Log	Entries (1-10 of 144 total)							Filter	Q,
5	All Dates	All En	forcers (1)	All Policies (1)	◄ All Lists (8)		•	All Reasons (2)	Reset
	DATE 😄	ENFORCER	POLICY 🖨	LISTS		REASON	PROTOCOL	ADDRESS	
>	03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +1		Country	TCP	103.190.91.21:80	
~	03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Talos IP RBL +3		Block List	TCP	95.128.43.164:80	=
	COUNTRY	ASN	REVERSE DNS		WHOIS			WHOIS.EXTENDED	
	Name FRANCE ISO Code 2 FR	Name Aqua Ray SAS ASN 41653	TTL 300 Class IN Record Type PTR Domain exit-1.fr.t	or.aquaray.com.	ISO Code 2 FR Description Tor servers Net Name AQUARAY-TOR	S-SERVERS		Autonomous System Name AQUARAY, FR Allocated 2009-01-20 Registry ripenco ISO Code 2 FR BGP Prefix 95.128.43.0/24 IP 95.128.43.164 Autonomous System # 41653	
>	03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +3		Block List	TCP	107.189.1.96:80	
>	03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +3		Block List	TCP	94.102.51.15:80	
>	03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +3		Block List	TCP	103.251.167.20:80	
>	03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Talos IP RBL +4		Block List	TCP	82.221.131.5:80	

Please note the following on the returned Log Entries:

- Reverse DNS and the basic WHOIS data may not be available for all entries
- It is common to find that some of the expanded data conflicts. For example, country and ASN
 information may differ across the various sources when expanded. These deltas can assist you when
 determining whether something is nefarious or not so that you can make a more informed decision
 about what you choose to allow.
- The "Existing Log Range", available in the status card above the table, provides the date range of logs that were available for that individual Enforcer. This range can be within or outside the search parameters. If the range available is outside the search parameters, the Log Entries table will still only display the results within the date range you originally searched for. You can use the "Existing Log Range" to determine if you may want to expand your search parameters.
 - Example: A log analysis is submitted for 03/07/24, 08:51 am to 03/07/24, 11:51 am. The "Existing Log Range" returned is 03/07/24, 03:00 am to 03/07/24, 11:51 am. The Log Entries table will only display Block IP entries on Ports 80 and 443 from 03/07/24, 08:51 am to 03/07/24, 11:51 am, if there are any that meet that criteria.
- A maximum of 1,000 entries per Enforcer will be returned.

- threatER Enforce software uses short-term RAM-based log storage to ensure the highest possible performance with no added latency to your network traffic while maintaining industry-leading security. Because of this and based on your network activity, your Enforce logs could wrap quickly and you may not be able to retrieve logs from within your specified time range.
 - For customers finding themselves constrained by these limitations, our strong recommendation is to leverage an external SIEM (such as Splunk, IBM Qradar, Gravwell, and others) to sink all logs using the Enforcer's built-in Syslog Export feature set, and then leverage the SIEM environment to perform unexpected blocks triage.

If an IP currently being blocked needs to be added to an Allow list:

- Scroll over the row that contains the IP
- Select the icon in the far-right column:

Log	Entries (1-10 of 144 total)						Filter	Q
5	All Dates	All Er	forcers (1)	All Policies (1)	All Lists (8)	•	All Reasons (2) -	Reset
	DATE 🖨	ENFORCER	POLICY	LISTS	REASON 🐡	PROTOCOL	ADDRESS	
>	03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +1	Country	TCP	103.190.91.21:80	
>	03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Talos IP RBL +3	Block List	TCP	95.128.43.164:80	(=,)
>	03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	► Block Blocklist.de +3	Block List	TCP	107.189.1.96:80	\smile
>	03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +3	Block List	TCP	94.102.51.15:80	

- Select the Allow list(s) to add the IP to
 - The colored pips next to the Allow list names indicate the following;
 - Green The list is enforced by the policy that blocked the IP address. Adding the IP to this List will allow it through the Networks Enforced by this policy.
 - Grey The list is not Enforced by the policy that blocked the IP address. If the IP is added to this List, the IP will be allowed on the Networks Enforced by the Policy(s).
 - Red The list is not enforced by any of your policies. If the IP is added to this List, it
 will continue to be blocked until and unless the list is added to policies of interest.
- Make any necessary edits to the IP entry:
 - Maskbits default is 32
 - Description default is "Added by Unexpected Blocks". We generally recommend that you update the description to be something meaningful such as tying it to a requesting end user, website, and/or discovery date.

- Expiration default is "Never"; however, we generally recommend that you time-bound allowed-lists additions when feasible.
- Click the "OK" Button

						<u>`</u>	
Log	Entries (1-10 of 1441	Allow Address 95.128.43.164				Filter	Q
5	All Dates	- Ö- Select which Allow Lists to	add IP Address	×	- A	All Reasons (2)	Reset
	DATE				PROTOCOL	ADDRESS	
>	03/05/24, 01:53 PM	ALLOW LIST	POLICIES	Maskbits 32	ТСР	103.190.91.21:80 💭	
>	03/05/24, 01:53 PM	Allow IP	None	Added by Unexpected Blocks	TCP	95.128.43.164:80 🔲	
>	03/05/24, 01:53 PM	Allow IP Inbound	Inbound Policy		TCP	107.189.1.96:80 🛛	
>	03/05/24, 01:53 PM	Allow IP Outbound	Outbound Policy	26 / 128 Expires	TCP	94.102.51.15:80 🗍	
>	03/05/24, 01:53 PM			Never Date/Time	TCP	103.251.167.20:80 🗌	
>	03/05/24, 01:53 PM				TCP	82.221.131.5:80 💭	
>	03/05/24, 01:53 PM			Cancel OK	TCP	185.220.101.38:80 🔲	
>	03/05/24, 01:53 PM	HQ Enforcer Outb	bound Policy Block T	Talos IP RBL Country	TCP	2.40.63.222:80 💭	

The IP is now added to the selected Allow list(s) and will be enforced by the policy(s) those lists are assigned to.

Reports

Reports provide a quick, graphical look at your system summaries. They contain metadata summarized from the detailed logs stored in Enforce. As no specific data is contained within the threatER portal, there should be no compliance issues.

To access Reports, select Enforce from the left-hand navigation menu and then select the Reports tab. The "Allowed/Blocked: Reason Summary" report is the default view. All data in reports is displayed in your browser's local time zone. There are 2 types of reports (Allowed/Blocked & Top 10) and each one has the functionality to schedule a report.

= threater						Q @ @	
E Collect							
Enforce	ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS	
🛧 Marketplace	Allowed / Blocked ©Times displayed	n timezone: America/New_York		Scheduled			
₄ ³ Messages	Reason Summary -	Last 30 minutes	- All Enforcers	✓ All Policies	- Reset		
Administration					1		
{} API Docs	Allowed by Reason 3 Total Allowed Connections			Blocked by Reason 367 Total Blocked Connections			
	10			400			
				200			
	succession			8 100 E			
	Connect			29 UUO O 40			
				20			
	1			10			
	Country	ASN	Allow List	Country	ASN Bloc	k List IP Reputation	

Allowed/Blocked

The Allowed/Blocked reports display the number of allowed or blocked connections for a given time frame, policy, and Enforcer. The default display for all Allowed/Blocked reports is all connections made in the last 30 minutes on all policies and Enforcers This data can be filtered based on a selection of preset timeframes, on a per policy basis, or on a per Enforcer basis.

This data is broken out into four separate reports, which are accessible via the drop-down at the top of the tab.

ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS
Ilowed / Blocked ©Times displayed	ed in timezone: America/New_York				Scheduled
Reason Summary	Last 30 minutes	✓ All Enforcers	✓ All Policies	- Reset	
Allowed / Blocked					
Allowed / Blocked: Reason Summary			Disclored by Desser		
Allowed / Blocked: Category Summary			Blocked by Reason 367 Total Blocked Connections	•	
Allowed / Blocked: Top 10 Countries			400		
Allowed / Blocked: Top 10 ASNs				_	
Top 10	-		200		
Top 10: Countries by Threat Category			5 100		
Top 10: ASNs by Threat Category			onnecti		
	-		3 40		
			20		
			10		
Country	ASN	Allow List	Country	ASN Bloc	k List IP Reputation

Reason Summary

The Allowed by Reason report displays connections that were allowed because of the following reasons (the below reasons are in the order the system processes enforcements):

- Allow List connections allowed based on explicit Allow list content
- ASN connections allowed by ASN adjustments
- Country connections allowed by a policy that were not specifically allowed by an Allow List or an ASN adjustment

The Blocked by Reason report displays connections that were blocked because of the following reasons (the below reasons are in the order the system processes enforcements):

- Block List connections blocked based on explicit Block list content
- IP Reputation connections blocked based on explicit Threat list content
- ASN connections blocked by ASN adjustments
- Country connections blocked by a policy that were not specifically blocked by a Block List

threateg

Allowed / Blocked ©Times displayed in timezone: America/New_York Reason Summary 	 ✓ All Policies ✓ Reset
Allowed by Reason 3 Total Allowed Connections	Blocked by Reason 367 Total Blocked Connections 400
Comeditions	200 100 40 40
1 Country ASN Allow List	20 Country ASN Block List IP Reputation

Clicking on a slice of data will open the Connection Detail for the report and display the following:

- Reasons and Count panel
 - Displays all reasons and the count for each
 - Default selection will be the reason selected on the previous graph
 - Selecting additional reasons will add that data to the graph on the right
- Total Blocked or Allowed Connections
- Top Reason Connections Blocked or Allowed
- Top Country Connections Blocked or Allowed
- Top ASN Connections Blocked or Allowed

Connection Detail La	st 30 minutes			Times display	ved in timezone: America/New_York
- REASON	COUNT	0.40	Block List	United States	Google LLC
Block List	270	349 Total Blocked Connections	Top Reason Connections	Top Country Connections	Top ASN Connections
IP Reputation	65		Blocked	Blocked	Blocked
Country	14				
☐ ASN	٥		109423 1109523 1100523 1100523 1100523 1100523 1100523 1100523 1100523 1100523 11005555555555555555555555555555555555		106823 1106023 1106023 1106023 066 PM 2:06 PM 2:10 PM 2:12 PM

Category Summary

The Allowed by Category report displays allowed connections that were indicated as part of a threat category, but fell below the configured thresholds for blocking at the time of connection.

The Blocked by Category report displays blocked connections that were found to be in a threat category at that time, regardless of why they were blocked and any blocking threshold.

Allowed / Blocked ©Times displayed in timezone: America/New_York Category Summary 	All Policies Feset
Allowed by Category ⁵ Total ⁹ ⁹ ⁹ ⁹ ⁹ ⁹ ⁹ ⁹	2,543 Total 106 106 106 106 106 106 106 106

Clicking on a slice of data will open the Connection Detail for the report and display the following:

- Threat category and Count panel
 - Displays the applicable threat categories and count for each
 - Default selection will be the category selected on the previous graph
 - Selecting additional categories will add that data to the graph on the right
- Total Blocked or Allowed Connections
- Top Reason Connections Blocked or Allowed
- Top Country Connection Blocked or Allowed
- Top ASN Connections Blocked or Allowed

threateg

THREAT	COUNT	704 700			
Endpoint Exploits	336,390	724,793 Total Blocked Connections	Endpoint Exploits Top Reason Connections	United States Top Country Connection	
Scanner	306,236		Blocked	Blocked	Blocked
Spam	54,436			<u> </u>	
Brute Force Password	7,841	Last 30 minutes			
Command and Control	6,119	15k			
Botnet	6,037	support to the second s			
Fraudulent Activity	3,647	5k			\mathbf{A}
DDOS	3,535				
Proxy / VPN	300		3/02/23 03/02/23 03/02/23 03/02/23 0 :50 PM 2:52 PM 2:54 PM 2:56 PM 2		3/02/23 03/02/23 03/02/23 03/02/23 03/02/23 :06 PM 3:08 PM 3:10 PM 3:12 PM 3:14 PM
P2P Node	217	Endpoint Exploits Botnet TOR / Anonymizer	→ Scanner -■ Spa → Fraudulent Activity -■ DDC → Compromised -■ Drop	S - Proxy / VPN	assword –∓ Command and Control –∓ P2P Node
TOR / Anonymizer	24				
Compromised	6				

Top 10 Countries

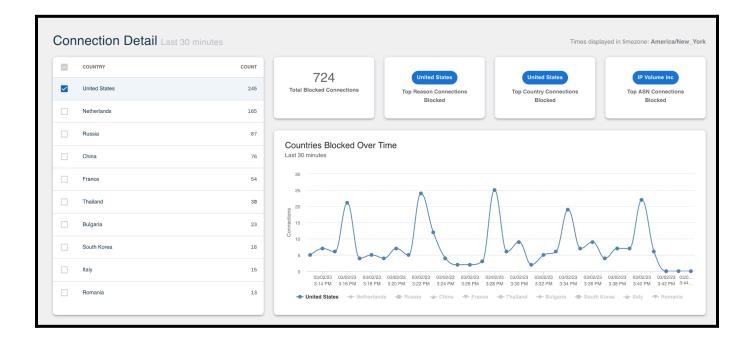
The Top 10 Countries report displays the countries the connections came from, based on what was allowed or blocked.

Allowed / Blocked ©Times displayed in timezone: America/New_York Top 10 Countries All Enforcers	All Policies Reset
Allowed by Country 952 Total Allowed Connections	Blocked by Country 1,066 Total Blocked Connections
RESERVED United States	South Kore Bulgaria Germany France United Kingdom Netherlands

Clicking on a slice of data will open the Connection Detail for the dashboard and display the following:

• Country and Count panel

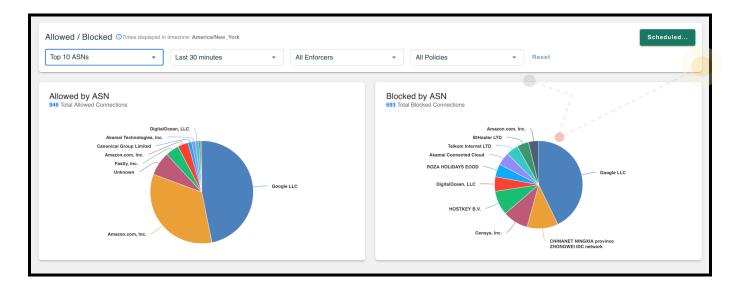
- Displays the applicable countries and the count for each
 - Default selection will be the country selected on the previous graph
- \circ $\;$ Selecting additional countries will add that data to the graph on the right
- Total Blocked or Allowed Connections
- Top Reason Connections Blocked or Allowed
- Top Country Connection Blocked or Allowed
- Top ASN Connections Blocked or Allowed



Top 10 ASNs

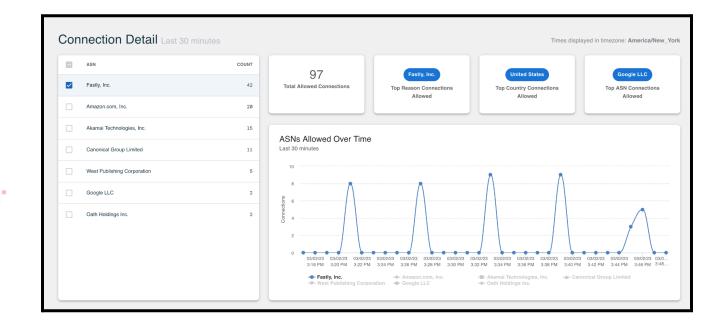
The Top 10 ASN report displays the ASNs the connections came from, based on what was allowed or blocked.

•



Clicking on a slice of data will open the Connection Detail for the dashboard and display the following:

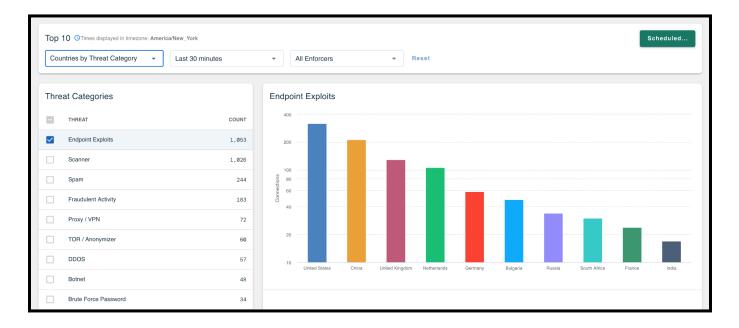
- ASN and Count panel
 - Displays the applicable ASNs and the count for each
 - Default selection will be the ASN selected on the previous graph
 - Selecting additional ASNs will add that data to the graph on the right
- Total Blocked or Allowed Connections
- Top Reason Connections Blocked or Allowed
- Top Country Connection Blocked or Allowed
- Top ASN Connections Blocked or Allowed



Top 10

Countries by Threat Category

The Top 10 Countries by Threat Category report displays graphs for the top 10 countries blocked due to specified threat category(s). These graphs can be accessed by selecting "Top 10: Countries by Threat Category" from the report drop-down.

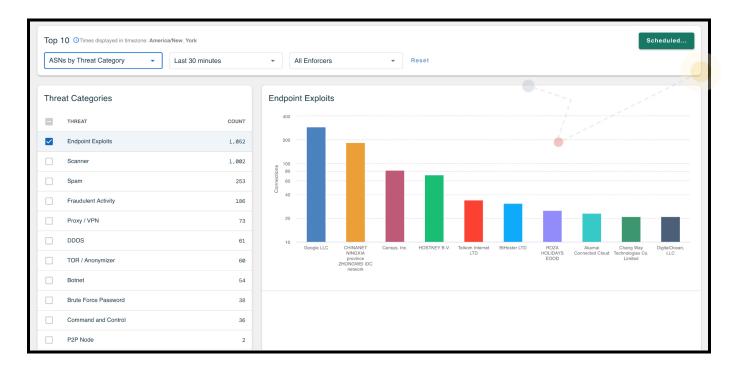


The Threat Category with the highest count will be selected by default and its graph will display in the right-hand panel. To view a graph for additional Threat Categories, select the desired category(s) in the left-hand panel.

Each threat category graph will display a bar for the top 10 countries with connections that have been flagged with that threat category. You can scroll over each bar to view the number of connections, based on the timeframe and Enforcer selected from the filters at the top of the screen.

ASNs by Threat Category

The Top 10 ASNs by Threat Category report displays graphs for the top 10 ASNs blocked due to specified threat category(s). These graphs can be accessed by selecting "Top 10: ASNs by Threat Category" from the report drop-down.



The Threat Category with the highest count will be selected by default and its graph will display in the right-hand panel. To view a graph for additional Threat Categories, select the desired category(s) in the left-hand panel.

Each threat category graph will display a bar for the top 10 ASNs with connections that have been flagged with that threat category. You can scroll over each bar to view the number of connections, based on the timeframe and Enforcer selected from the filters at the top of the screen.

Scheduled Reports

Users can set a schedule for all reports. These reports will be emailed based on the schedule selected and the email will include a link to access the report by way of the threatER portal.

Reports can be scheduled by:

• Selecting the "Scheduled" button in the top-right corner of a report

ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS
Allowed / Blocked ©Times display Reason Summary		 All Enforcers 	✓ All Policies	- Reset	Scheduled
Allowed by Reason 3 Total Allowed Connections			Blocked by Reason 377 Total Blocked Connections		
			130		
Connections			115		_
1 Country	ASN	Allow List	110 Country	ASN Block List	IP Reputation

• Select the Create button in the top right corner

	ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPOR	ITS
Scheo	duled Reports (1-1 total)						Create
All Rep	orts 👻					Filter	Q
•	NAME	REPORT	LAST RUN 👙	NEXT RUN 👙	DESCRIPTION		
•	Allowed - Blocked Report	Allowed / Blocked: Reason Summary	11/07/23, 12:00 AM	11/08/23, 12:00 AM	Daily report of what was allowed and block	ed the previous day	:
					PER PAGE: 20 🔻	1-1 total < PREVIOUS	1 NEXT >

- Selected the Report type
- Provide the following details (* indicates required field):
 - *Name
 - *Delivery Email
 - This is the email the link to the report will be sent to
 - Description
 - *Preset
 - Select one of the following from the drop-down:
 - Yesterday report will run daily at midnight and includes data from the previous 24 hours
 - Last Week report will run weekly at midnight on Sunday and includes data from the previous week

- Last Month report will run monthly at midnight on the 1st of each month and includes data from the previous month
- Last 7 days report will run daily at midnight and includes data from the previous 7 days
- Policy (parameter only available for Allow/Blocked reports)
 - All Policies is the default selection
 - An individual policy can be selected from the drop-down
- *Threat Categories (parameter only available for Top 10 reports)
 - From the drop-down, select the desired Threat Categories to include in the report
- All Enforcers is the default selection
 - An individual Enforcer can be selected from the drop-down
- Select the Create button

Create Scheduled Report		
Enabled		
Report		•
Name		
		0 / 64
Delivery Email		
Description		
		0 / 128
Preset Select Preset		•
Timezone America/New_York		
	Cancel	Create

The report will be emailed to the address provided, based on the parameters selected.

Editing Scheduled Reports

.

To update the parameters of a scheduled report:

• On the Report tab, select the Scheduled button

ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS
Allowed / Blocked ©Times d Reason Summary	isplayed in timezone: America/New_York Last 30 minutes	✓ All Enforcers	✓ All Policies	Reset	Scheduled
Allowed by Reason 2 Total Allowed Connections			Blocked by Reason 416 Total Blocked Connections		
Connections			Oonnections		
1 Country	ASN	Allow List	100 90 80	ASN Block Li	it IP Reputation

• Select Edit from the ellipsis menu in the row of the report you would like to edit

	ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPOR	тѕ
Sched	uled Reports (1-1 total)						Create
All Repo	orts 👻					Filter	Q
÷	NAME 🗇	REPORT 🖨	LAST RUN 👙	NEXT RUN 👙	DESCRIPTION		
-	Allowed - Blocked Report	Allowed / Blocked: Reason Summary	11/07/23, 12:00 AM	11/08/23, 12:00 AM	Daily report of what was allowed and block	ed the previous c Edit	:
					PER PAGE: 20 👻	1-1 total < PR	T >

• Make the desired updates and then select the Save button

Edit Scheduled Report
Enabled
Report Allowed / Blocked: Reason Summary
Name Allowed - Blocked Report
24/64
Delvery Email companymasteruser@valuedcustomer.com
Description Daily report of what was allowed and blocked the previous day
61/128
Policy
All Policies
Enloreer
All Enforcers +
Preset
Yesterday -
The 'Yesterday' preset runs daily at midnight, includes data from the previous 24 hours'
Timezone America/New_York
Cancel Save

Disabling Scheduled Reports

To disable a scheduled report:

- On the Report tab, select the Scheduled button
- In the row of the desired report, position the toggle to the left
- On the Disable Scheduled Report confirmation modal, select the Disable button

	ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORTS
Sched All Rep	duled Reports (1-1 total) orts					Create Filter Q
÷	NAME		LAST RUN 🖨	NEXT RUN 👙		
	Allowed - Blocked Report	Allowed / Blocked: Reason Summary		11/08/23. 12:00 AM	Daily report of what was allowed and blocke	ad the previous day
		Disable Sched	uled Report	_	PER PAGE: 20 👻	1-1 total < PREVIOUS 1 NEXT >
			you want to Disable this Sche	duled Report?		
		Allowed - Block	ed Report			
			c	Cancel Disable		

The report is now disabled and will no longer be emailed to the address that was provided.

To enable the report at a later date, position the toggle to the right and confirm the action.

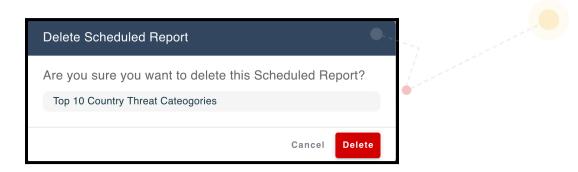
Deleting Scheduled Reports

To delete a scheduled report:

- On the Report tab, select the Scheduled button
- Select Delete from the ellipsis menu in the row of the report you would like to delete

	ENFORCERS	NETWORKS	PORTS	POLICIES	SUBSCRIPTIONS	REPORT	S
Scheo	duled Reports (1-2 total)						Create
All Rep	ports 👻					Filter	Q
	NAME 🗇	REPORT	LAST RUN	NEXT RUN 🖨	DESCRIPTION		
	Allowed - Blocked Report	Allowed / Blocked: Reason Summary	11/07/23, 12:00 AM	11/08/23, 12:00 AM	Daily report of what was allowed and blog	ked the previous day	:
	Top 10 Country Threat Cateogories	Top 10: Countries By Threat Category	-	-	•	Edit	:
					PER PAGE: 20 👻 1	-2 total < PR	>

• On the Delete Scheduled Report confirmation modal, select the Delete button

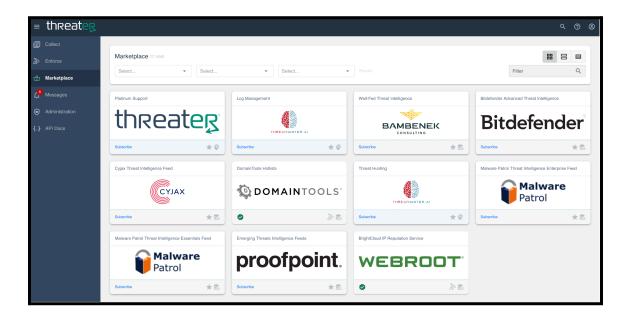


The report is now deleted, will not display in the Scheduled Reports table, and will no longer be emailed.

Marketplace

The Marketplace provides threatER customers access to high-value, multi-source cyber intelligence data from leading intelligence providers, as well as services to help manage and resolve threats in your network. Our Marketplace includes offerings from longtime partners, premium offerings from new partners, and an expanded partnership with DomainTools.

To access these offerings, select Marketplace from the left-hand navigation menu. All available products will display.



Included with Enforce Products

Some products, such as DomainTools and Webroot, are available to Enforce customers at no additional cost and display a "Included with Enforce" glyph on the card. There is no need to subscribe to these products and the feeds associated with these products are available to you and accessible via Collect.



Premium Intelligence Products

You may choose to purchase supplemental premium cyber intelligence feeds that are not included with your Enforce subscription. The pricing of these products is based on the total number of Enforcers on your account.

To purchase a product:

• Select the product from the list



- Review the terms of the subscription provided on the next screen
- Select the Terms and Conditions hyperlink (if applicable) to review in a separate tab
- Select the Terms and Conditions checkbox to enable the Add Product button
- Select the Add Product button

Well-Fed Threat Intelligence	
Description	Pricing Summary
Well-Fed Threat Intelligence is produced by Bambenek Consulting, LTD. Bambenek is a leading cybersecurity threat intelligence and data science firm led by industry veteran John Bambenek.	Monthly Subscription Cost \$139.90 Number of Enforce Subscriptions x 1
Well-Fed operates one of the largest repositories of curated threat intelligence that is publicly available. Using novel techniques, Well-Fed threat intelligence is generated by surveilling attackers to see where they actually live so you have the latest information to protect yourself. Approximately one million malicious domains are monitored every hour and are curated and whitelisted to ensure that you have the reliable information you need to protect yourself from cybercriminals. Well-Fed Threat Intelligence is used by thousands of organizations all over the world to protect themselves and their customers.	Total Price \$139.90
The Well-Fed Intelligence subscription offering provides access to three distinct threat feeds including:	Add Product
Sinkhole IP Feed - a manually curated list of over 1,500 known sinkholes.	Access to the applicable intelligence product(s) will be effective
DGA Feed - a self-curating feed that monitors malicious networks to observe current criminal activity. This is live data of between 750 and 1,500 domains, which are used by 65 matware families and nearly 1 million domains.	immediately. Your account will be invoiced, based on the subscription term and amount shown in the Pricing Summary.
MaldomainML - a feed based on proprietary machine learning and analytical methods of DNS telemetry developed in Bambenek Labs. Provides protection from malware and phishing domains.	

A modal will display providing further details about the subscription, to include the feeds you now have access to. Review these details and then select the OK button to close the modal. You will be redirected to the full list of Marketplace products. The product will now display as Subscribed.

Services

The threatER Marketplace included Services products that help manage and resolve threats in your network.

To request a quote on any of these services:

- Select "Services" from the Products drop-down
 - This will narrow down the available options to our Services products

= threater								۹	0	٩
E Collect										
Enforce	Marketplace (11 total, 3 filtered)				л			88 8		
🕁 Marketplace	Services Select	Select	▼ Select	•	Reset		 Filter		Q	
4 ¹² Messages	Intelligence		Log Management		Threat Hunting					
Administration			4							
{} API Docs	threat		THREATHUNTER.AI		THREATHUNTER. AI					
	Subscribe	* 9	Subscribe	* 🛛	Subscribe	* 🛛				

- Click on a Service to view more information
- Click the "Get a Quote" button to submit your interest in this service

= threater			Q (2	
 □ Collect > Enforce → Marketplace 	Log Management advanced data handling, analysis, and insights	THREATHURTER.AI		
L ¹² Messages	Description Need to go deeper into your data for advanced analysis and insights? Threater's partnership with ThreatHunter allows just that. The LogLlama Core package is tailored for businesses that need robust data handling capabilities. If you're ready to do more with your log data, reach out today and someone will be in touch to get you started.	Pricing Summary Monthly Subscription Cost Starting at \$ Get a Quote	\$60.00 per i	nonth
	Partner ThreatHunter.ai, a 100% Service-Disabled Veteran Owned Small Business, specializes in advanced threat detection and response, utilizing AI and machine learning to combat cyber threats. The firm is known for its AI-driven threat detection platform, integrating seamlessly into security systems for real-line threat analysis. With a mission to provide intelligent, automated cybersecurity solutions, ThreatHunter.ai is at the cutting edge of technology and cyber intelligence.			

After your request is submitted, someone from our team will contact you to discuss the necessary details and onboard the service to your account.

Ó

Administration

Users

The Users tab displays all users for your company and is where you can create new users, edit existing user accounts, enable/disable user accounts, and delete user accounts. To view your company's users, select Administration from the left-hand navigation menu and then select the User tab.

= threater						0	
E Collect	USERS	SUBSCRIPTIONS	COMMAND LOGS	ENFORCE DOWNLOADS			
会 Marketplace 슈 ³ Messages	Users (1-3 total) All Roles			Filter	Cr	eate Q	
Administration	⇔ EMAIL ⇔		IDENTITY PROVIDER 🌐	ROLE 🔤			
{} API Docs	companyreadonly@valuedcustomer.c	om	THREATER	Company Read Only		:	
	companymasteruser@valuedcustome	.com	THREATER	Company Master		:	
	companyhelpdeskuser@valuedcustor	her.com	THREATER	Company Help Desk		:	
				PER PAGE: 20 - 1-3 total < PREVIOUS	1 NE	XT >	

Please refer to the Appendix for an overview of what actions each user role can perform within the admin console.

Create New User

Company Master users can create new users by completing the following steps:

- Select the Create button in the top right corner of the Users table
- Enter the user's email address
- Select a Role from the drop-down
- Select the Create button

USERS	SUBSCRIPTIONS	COMMAND LOGS	ENFORCE DOWNLOADS
Users (1-3 total) All Roles		Create Filter Q	
🗢 EMAIL 😄	IDENTITY PROVIDER	ROLE 🐡	Email companyadmin@valuedcustomer.com
companyreadonly@valuedcustomer.com	THREATER	Company Read Only	
companymasteruser@valuedcustomer.co	DM THREATER	Company Master	Select Role Company Admin
companyhelpdeskuser@valuedcustomer	.com THREATER	Company Help Desk	
	PER PAGE: 20 👻	1-3 total < PREVIOUS 1 NEXT >	Cancel Create

The new user will be created and an Account Activation email will be generated to the email provided. This email will contain the link for the user to complete the setup of their threatER account.

Edit User Accounts

Disable an Account

To disable an account:

- Search for the user account that needs to be disabled
- Position the Enable toggle to the left

USERS SUBSCRIPTIONS		COMMAND LOGS	ENFORCE DOWNLOADS	ENFORCE DOWNLOADS		
Users All Role	i (1-4 total) es -			Filter	Create Q	
÷	EMAIL		IDENTITY PROVIDER			
-	companyadmin@valuedcustomer.com		THREATER	Company Admin	0 0 0	
	companyreadonly@valuedcustomer.com		THREATER	Company Read Only	* *	
	companymasteruser@valuedcustomer.com		THREATER	Company Master	* *	
•	companyhelpdeskuser@valuedcustomer.com	n	THREATER	Company Help Desk	* *	
				PER PAGE: 20 👻 1-4 total < PREVIOUS	NEXT >	

• On the Disable User confirmation modal, select the Disable button



Disable User		
Are you sure you want to Disable this User?	•	
companyadmin@valuedcustomer.com		
Cancel	Disable	

The user is now disabled and will not be able to log into the portal.

Enable an Account

To enable an account:

- Search for the user account that needs to be enabled
- Position the Enable toggle to the right

Users (1-4 (otal)		Create
All Roles -		Filter Q
⇔ EMAIL ⇒	IDENTITY PROVIDER	ROLE 🗇
companyadmin@valuedcustomer.com	THREATER	Company Admin
companyreadonly@valuedcustomer.com	THREATER	Company Read Only
companymasteruser@valuedcustomer.com	THREATER	Company Master
companyhelpdeskuser@valuedcustomer.com	THREATER	Company Help Desk
		PER PAGE: 20 👻 1-4 total < PREVIOUS 1 NEXT >

• On the Enable User confirmation modal, select the Enable button

Enable User
Are you sure you want to Enable this User?
companyadmin@valuedcustomer.com
Cancel

Update User Email

To update a user's email address:

- Search for the user account
- From the ellipsis menu in the right-hand column of the row, select Edit
- Edit the Email field
- Select Save

Users (1-4 total)			Create	Edit User
All Roles		Filter	Q	Enabled
	IDENTITY PROVIDER	ROLE 🖨		Email companyadmin@valuedcustomer.com
companyadmin@valuedcustomer.com	THREATER	Company Admin	:	
companyreadonly@valuedcustomer.com	THREATER	Company Read Only	:	Select Role Company Admin
companymasteruser@valuedcustomer.com	THREATER	Company Master	:	
companyhelpdeskuser@valuedcustomer.com	THREATER	Company Help Desk	:	Password
	PER PAGE: 20 👻	1-4 total < PREVIOUS	NEXT >	Leave Password fields blank to keep current Password
				Confirm Password
				Leave Password fields blank to keep current Password
				Cancel Save

The user's email address is now updated and this is the username the user needs to use when logging into the portal.

Update User Role

To update a user's role:

- Search for the user account
- From the ellipsis menu in the right-hand column of the row, select Edit
- Select the desired role from the Role drop-down
- Select Save

Users	\$ (1-4 total)			Create	Edit User
All Role	es 👻		Filter	Q	Enabled
	EMAIL 🕀	IDENTITY PROVIDER	ROLE		Email companyadmin@valuedcustomer.com
	companyadmin@valuedcustomer.com	THREATER	Company Admin	:	
•	companyreadonly@valuedcustomer.com	THREATER	Company Read Only	:	Select Role
	companymasteruser@valuedcustomer.com	THREATER	Company Master	:	Company Read Only
	companyhelpdeskuser@valuedcustomer.com	THREATER	Company Help Desk	÷	Company Help Desk
		PER PAGE: 20 👻	1-4 total < PREVIOUS 1	NEXT >	Company Admin
					Company Master
					Leave Password fields blank to keep current Password
					Cancel Save

NOTE: please refer to the Appendix for an overview of what actions each user role can perform within the admin console.

Update User Password

To update a user's password:

- Search for the user
- From the ellipsis menu in the right-hand column of the row, select Edit
- Enter the new password in both the Password and Confirm Password fields
- Select Save

II Roles -		Filter	Q	Enabled
EMAIL 👙	IDENTITY PROVIDER	ROLE		- Email companyadmin@valuedcustomer.com
companyadmin@valuedcustomer.com	THREATER	Company Admin	:	
ocompanyreadonly@valuedcustomer.com	THREATER	Company Read Only	:	Select Role Company Admin
companymasteruser@valuedcustomer.com	THREATER	Company Master	:	
companyhelpdeskuser@valuedcustomer.com	THREATER	Company Help Desk	:	Password
	PER PAGE: 20	▼ 1-4 total < PREVIOUS	1 NEXT >	Leave Password fields blank to keep current Password
				Leave Password fields blank to keep current Password

The user's password is now updated and this is the password the user will need to use when logging into the portal.

Delete Users

To delete a user:

- 1. Search for the user
- 2. From the ellipsis menu in the right-hand column of the row, select Delete
- 3. On the Delete User confirmation modal, select the Delete button

Delete User	
Are you sure you want to delete this User?	
companyreadonly@valuedcustomer.com	
Cancel	Delete

The user is now deleted and will not be able to access the admin console.

Users Filter

You can filter down to a user or set of users in the following ways:

- All Roles Selecting a user role from this drop-down will filter the table down to the users who are assigned the selected role.
- User Table Filter Enter text in the Filter Table search bar in the top right corner of the screen and the table will update to display applicable results.

II Roles	⊗ ^		Filter	C
All Roles		IDENTITY PROVIDER 🌐	ROLE	
Company Read Only Company Help Desk	er.com	THREATER	Company Admin	
Company Admin	omer.com	THREATER	Company Read Only	
Company Master	stomer.com	THREATER	Company Master	
companyhelpdeskuse	er@valuedcustomer.com	THREATER	Company Help Desk	

Subscriptions

The Subscriptions tab displays all threatER subscriptions that have been purchased. This includes Enforce

and Marketplace subscriptions.

USERS	SUBSCRIPTIONS	COMMAND LOGS	ENFORCE DOWNLOAD	s
Subscriptions (1-8 total)				
All Types 👻			Filter	Q
NAME 😄			туре 😋	ENFORCE
Enforce Subscription			Enforce	HQ Enforcer
Enforce High Availability Subscription			Enforce	•
Enforce Subscription			Enforce	-
Bitdefender Intelligence Subscription 3Gb			Marketplace	÷
Cyjax Intelligence Subscription			Marketplace	•
DomainTools IP Hotlist			Marketplace	•
Malware Patrol Enterprise Cyber Intelligence Subscription			Marketplace	-
WELL-FED Intelligence Subscription 3Gb			Marketplace	-
			PER PAGE: 20 - 1-8 total < PREVIO	

Command Logs

Command logs show a history of important actions taken by users of the system. These can be useful for auditing and troubleshooting any issues that arise.

threater	_							৭ 💿
		USERS	su	IBSCRIPTIONS		COMMAND LOGS	ENFORCE DOWNLOADS	
Marketplace Messages	Comman	d Logs					Search	Q
Administration	DATE -	USER	INITIATOR	MODULE	ACTION	MESSAGE		
API Docs	11/07/23, 10:49:02	companymasteruser@valuedcustomer.com	User	User	Update	companymasteruser@valuedcustomer.com: User "companya	dmin@valuedcustomer.com" modified: 'active' => 'True	
	11/07/23, 10:47:49	companymasteruser@valuedcustomer.com	User	User	Update	companymasteruser@valuedcustomer.com: User "companyae	dmin@valuedcustomer.com" modified: 'active' => 'False	e' (was 'True')
	11/07/23, 10:46:09	companymasteruser@valuedcustomer.com	User	User	Update	companymasteruser@valuedcustomer.com: User "companyadmin@valuedcustomer.com" modified: 'email' => 'companyadmin@valuedcustomer.com' (was 'marie.knight+userguideadmin@threater.com)		
	11/07/23, 10:45:53	companymasteruser@valuedcustomer.com	User	User	Delete	companymasteruser@valuedcustomer.com: User deleted - en Guide, role: CMP_READONLY	nail: marie.knight+userguide@threatblockr.com, compa	any: Threater
	11/07/23, 10:45:48	companymasteruser@valuedcustomer.com	User	User	Delete	companymasteruser@valuedcustomer.com: User deleted - en CMP_ADMIN	nail: marie.knight@threater.com, company: Threater Gi	uide, role:
	11/07/23, 10:36:37	companymasteruser@valuedcustomer.com	User	User	Create	companymasteruser@valuedcustomer.com: User created - en Guide, role: CMP_READONLY	mail: marie.knight+userguide@threatblockr.com, compa	any: Threater
	11/07/23, 10:35:53	companymasteruser@valuedcustomer.com	User	User	Create	companymasteruser@valuedcustomer.com: User created - er CMP_ADMIN	nail: marie.knight@threater.com, company: Threater G	uide, role:
	11/07/23, 10:34:56	companymasteruser@valuedcustomer.com	User	User	Create	companymasteruser@valuedcustomer.com: User created - er Guide, role: CMP_ADMIN	nail: marie.knight+userguideadmin@threater.com, com	pany: Threater
	11/07/23, 10:24:38	companymasteruser@valuedcustomer.com	User	Report Schedule	Delete	companymasteruser@valuedcustomer.com: Scheduled report	"Top 10 Country Threat Cateogories" deleted	
	11/07/23, 10:23:04	companymasteruser@valuedcustomer.com	User	Report Schedule	Create	companymasteruser@valuedcustomer.com: Scheduled report	"Top 10 Country Threat Cateogories" created	
	11/07/23, 09:29:26	companymasteruser@valuedcustomer.com	User	Report Schedule	Delete	companymasteruser@valuedcustomer.com: Scheduled report	"Country Top 10 Report" deleted	
	11/04/23, 11:01:40	companymasteruser@valuedcustomer.com	User	Policy	Delete	companymasteruser@valuedcustomer.com: Deleted policy "N	lew Policy*	

IOC Search

The Indicator of Compromise (IOC) Search allows users to search any IP address or domain to see if it is a malicious actor found in any of our threatERr-provided Threat or Block feeds. Available information about the country and ASN, when available, are returned as well.

To perform a search:

- Select the spyglass icon in the top navigation bar
- Enter an IP address or domain
- Select the search icon in the modal

= thre	ateg											
Collect												
➢ Enforce				LISTS						MARKET	IPLACE	
🕁 Marketplace	,	Lists (1-58 of 58 total)										Create
⊥ Messages		All Types	~ Al	I Health States	-	All Indicators	-	All Sources	-	All Access	- Reset Filter	Q
) Administrati	on	NAME 😄	TYPE 😄		SOURCE 🖨	ACCESS 👙	POLICIES 🕀	COUNT 🖨		LAST UPDATE	DESCRIPTION	G
{} API Docs		Akamai	Allow	IP	CSV File Connec	tor Public	Outbound	19	11/07/23, 11:34 AM	02/13/23, 04:34 PM	Akamai curated by Greynoise	
		AlienVault OTX	Block	IP / Domair	Indicator Sea	arch				1/07/23, 0:30 AM	AlienVault OTX	
		Allow	Allow							0/25/23, 0:10 AM		
		Amazon Cloudfront	Allow	107.178.223	183			Q	Search	7/10/23, 6:09 PM	Amazon Cloudfront curated by Greynoise	
		Bambenek DGA	Block							1/07/23, 1:17 AM	Domain Generation Algorithm IP feed	
		Bambenek DGA	Block	Domain	Bambenek	Public	 Allow All Int +2 	576,028	11/07/23, 11:28 AM	11/06/23, 10:15 PM	Domain Generation Algorithm Domain feed	

The results that display will provide general information on the IP or domain.

IP / Domain Indicator	Search			×
107.178.223.183			Q	Search
General Info				^
ADDRESS	COUNTRY	ASN	BLOCK LIST	THREAT LIST
107.178.223.183	United States	Google LLC	\oslash	\oslash
Block List History [7]			~
Threat List History (458]			~

If the indicator has history on any Threat or Block feeds provided by threatER, this will be included and the section can be expanded to view those details.

Users can also perform the search by selecting the hyperlinked IP address or domain within a threatER-provided feed.

User Profile

The User Profile is where users can update their contact information, change their password, generate an API Key, and enable Multi-Factor Authentication.

The User Profile is accessible by selecting the person icon in the top-right navigation bar and then selecting User Profile.

= threater				۹ 🕲 😣
E Collect				Logged in as companymasteruser@valuedcustomer.com
Enforce	USERS			User Profile
🕁 Marketplace	User Profile			Company Profile
🔏 Messages	User Details			Edit Profile Change Password
Administration	FIRST NAME	LAST NAME	MOBILE PHONE NUMBER	EMAIL companymasteruser @valuedcustomer.com
{} API Docs	COMPANY Threater Guide	COMPANY UUID 09F120E1-409C-44D5-8E69-6337089E20E6	ROLE Company Master	
	API API Key RQ20WTK09474U5XNMJVD Secret Beth an API key and secret are needed. If you lose it, you	e.	Multi-Factor Authentication 1. Get the App Download and install the Google Authenticator, Authy, 2. Gath Be Brack Open the sufferification app and: • Tap the ** loan the top-right of the app • San the image to the right using your phone's car Can't scan this barcode? Direc the barcode above is scanned, enter the 6-digit of	

User Details

The User Details section is where users can view and edit their profile details. To edit your profile:

- Select the Edit Profile button
- Enter the following optional information:
 - First Name
 - Last Name
 - Phone Number
- Select Save

			Edit Profile Change Password
Edit Profile	4	EMAIL	iser@valuedcustomer.com
First Name Jane	0		
Last Name Doe	4/64	thentication	MFA is inactive for your account
	3/64		
5557779999	8	all the Google Authenticator, Authy, or windows Phore	he Authenticator app for your phone or tablet.
	Cancel Save	ation app and: I in the top-right of the app	
	First Name Jane Doe Phore Namber 5557779999	First Name Image: Constraint of the second sec	Edit Profile companymaters In the top-right of the app Cancel Save Link to the top-right of the app Cancel Save Link to the top-right of the app

Email and Role updates cannot be made on the User Profile. To update either of these, please contact your Company Master account.

API Key

If API Access is allowed for your company, you can generate an API Key for API endpoint authorization.

To generate an API Key, select the Generate button in the API Key section.

User Profile			
Jane E COMPANY C	AST NAME See COMPANY UUID 99F120E1-400C-4405-8E89-0537089E20E6	MOBILE PHONE NUMBER - ROLE Company Master	Edit Profile Change Password EMAIL companymasteruser@valuedoustomer.com
API API Key Secret Both an API key and secret are needed. If you lose it, you will need to re	8	Multi-Factor Authentication 1. Get the App Download and install the Google Authenticator, Authy 2. Scan this Barcode Open the authentication app and: • Tap the "+" icon in the top-right of the app • Scan the image to the right, using your phone's ce Can't scan this barcode? 3. Enter Verification Code Once the barcode above is scanned, enter the 6-digit	

An API Key and Secret will be generated. Both are needed and should be maintained securely for API use. If the API Key and Secret are lost at any point, a new one will need to be generated.

If API Access is not enabled for your company, this section will not display on the User Profile. If API Access is desired, please contact your Company Master account.

Multi-Factor Authentication (MFA)

MFA for Individual Account

MFA can be enabled for your individual account, if it is not required by your company by default.

To enable MFA for your account:

- Download and install one of the following apps on your phone or tablet:
 - Google Authenticator

- Twilio Authy
- Windows Phone Authenticator
- Open the app of your choice and scan the barcode on the User Profile screen using the camera on your phone or tablet.

Ó

• Enter the Verification Code and select the Activate button

MFA is now active for your account and will be reflected as so on your User Profile. When logging in from this point forward, you will be prompted to enter a passcode after entering a valid username and password.

User Profile			
User Details			Edit Profile Change Password
FIRST NAME Jane COMPANY Threater Guide	LAST NAME Doe COMPANY UUID 09F120E1-409C-44D5-8E69-6337089E20E6	MOBILE PHONE NUMBER - ROLE Company Master	EMAIL companymasteruser@valuedcustomer.com
API API Key	Generate	Multi-Factor Authentication	MFA is active for your account
RQ20WTK09474U9XNMJVD			Deactivate
Secret			
	<i>©</i>		
Both an API key and secret are needed. If you lose it, you will	need to generate a new API key and secret.		

When MFA is active, you will be prompted to provide a code from the authentication app you used to activate MFA each time you login to the portal.

Deactivate MFA

If MFA is not required by your company, you can deactivate it for your individual account. To deactivate MFA:

- Navigate to your User Profile
- Selecting the Deactivate button in the MFA panel

User Profile			
User Details			Edit Profile Change Password
FIRST NAME Jane	LAST NAME Doe	MOBILE PHONE NUMBER	EMAIL companymasteruser@valuedcustomer.com
COMPANY Threater Guide	COMPANY UUID 09F120E1-409C-44D5-8E69-6337089E20E6	ROLE Company Master	
API	Gener	Multi-Factor Authentication	MFA is active for your account
API Key			Deactivate
RQ20WTK09474U9XNMJVD			
Secret			
		ø	
Both an API key and secret are needed. If you lose	it, you will need to generate a new API key and secret.		

• On the Delete MFA confirmation modal, select the Delete button

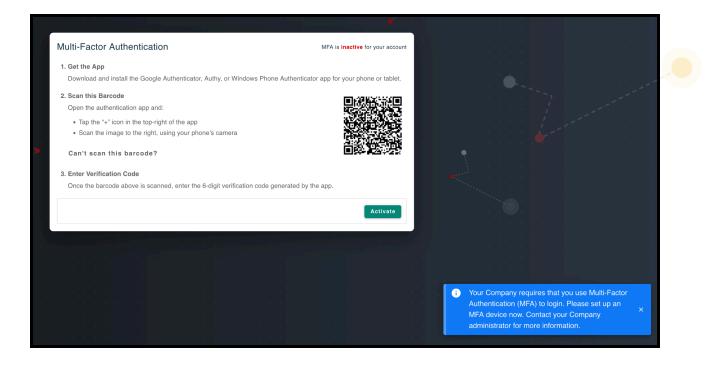
Delete Multi-Factor Authentication Device	
Are you sure you want to deactivate MFA?	
Cancel	Delete

MFA is now inactive for your account. The next time you login to the portal you will not be prompted to enter a passcode.

MFA Required by Company

If MFA is required by your company, you will be required to set up MFA for your account.

After entering your username and password and selecting Sign On on the login screen, you will be directed to set up MFA for your account.



- Download and install one of the following apps on your phone or tablet:
 - Google Authenticator
 - Twilio Authy
 - Windows Phone Authenticator
- Open the app of your choice and scan the barcode on the User Profile screen using the camera on your phone or tablet
- Enter the Verification Code and select the Activate button

MFA is now active for your account and will be reflected to the login screen. After entering a valid username and password, you will be prompted to enter a passcode from the authentication app. For every future login you will be prompted to enter a passcode after entering a valid username and password.

Company Profile

The Company Profile is only accessible to Company Master accounts and is where company-level settings can be made.

The Company Profile is accessible by selecting the person icon in the top-right navigation bar and then selecting Company Profile.

threateg

Single Sign-On (SSO)

If your company subscribes to Google Workspace and your company's domain is registered to Google Workspace, you can now log into the portal via SSO with Google. In addition to the standard SSO, Company Master accounts can configure your company to allow for new user creation via SSO. Properly configuring this setting allows new users to be created via SSO on the login screen when matched to one or more allowed domains.

Note that most customers will likely **not** want to enable this feature, since anyone with a valid domain credential would be able to log into the system, which is often undesirable for access to security controls such as threatER. However, it may be useful for some security organizations to allow employees to have the ability to create accounts quickly without having to bother a Company Master to do so.

To allow new users to be created via SSO, a Company Master should:

- Navigate to the Company Profile
- Toggle On the "Allow SSO to Create New Users" setting
- Select the User Role the new user will be created as
 - Read Only is strongly recommended
 - User permissions can be updated at a later time

ingle Sign-On		
llow SSO to Create New Users	Add Login Domain	
•	host.com	Add
reate New Users with Role	Login Domains	
Company Read Only	valuedcustomer.com	Ē
Select Role		
Company Read Only		
Company Help Desk	Multi-Factor Authentication	
Company Admin	Require Multi-Factor Authentication	
Company Master Admin	-	

- Enter the applicable email domain(s). Anyone with a valid login to the specified domain as registered with the SSO provider (in this case, the associated Google Workspace domain) will be able to create an account on the system.
- Select the Add button

Single Sign-On		
Allow SSO to Create New Users	Add Login Domain	
•	valuedcustomer.com	Add
Create New Users with Role	Login Domains	
Company Read Only	✓ No Login Domains	
ÀPI	Multi-Factor Authentication	
Niow API Access	Require Multi-Factor Authentication	
NIOW AFT ACCESS		

• Select Save

Once this setting is properly configured, the Company Master can direct their new users to:

- Navigate to the login screen
- Select "Sign On with Google"
- Follow the prompts

API

To allow users to use the portal API endpoints, Company Masters must turn on API access. To do this, a

Company Master should:

- Navigate to the Company profile
- Toggle on "Allow API Access"
- Select the Save button in the top right corner

Company Profile Threater Guide		Reset Save
Single Sign-On Allow SSO to Create New Users	Add Login Domain	Add
Create New Users with Role Company Read Only	Login Domains valuedcustomer.com	
API	Multi-Factor Authentication	
Allow API Access	Require Multi-Factor Authentication	

Each user will now have the ability to generate an API Key on their individual user profile. The generated API Key will give the user access to the API endpoints with the permissions their account is setup with (i.e. Company Help Desk).

Multi-Factor Authentication (MFA)

Company Masters can choose to require all users of their company to use MFA when logging in. To require MFA for your company, a Company Master should:

- Navigate to the Company Profile
- Toggle on "Require Multi-Factor Authentication"
- Select the Save button in the top right corner

Company Profile Threater Guide		Reset	Save
Single Sign-On Allow SS0 to Create New Users	Add Login Domain		
	host.com		Add
Create New Users with Role	Login Domains		
Company Read Only	valuedcustomer.com		Ō
API	Multi-Factor Authentication		
Allow API Access	Require Multi-Factor Authentication		

All users of your company will be required to set up MFA for their account. Please see the MFA Required by Company section for additional details.

Appendix

User Roles and Permissions

User Roles and Pe	ermissio	าร			
	CMP Roles & Permissions			•	
	Read Only	Help Desk	Admin	Master	
	COLL	ECT			
LISTS					
View Lists	х	х	Х	х	
Create Lists			Х	x	
Edit Lists			Х	х	
Delete Lists			Х	x	
MARKETPLACE					
View Products	x	х	Х	x	
View Product Details	x	х	Х	x	
Subscribe to a Product				x	
	ENFO	RCE			
ENFORCERS					
View Enforcers	x	х	Х	x	
Edit Enforcer Name/Location			Х	х	
Manage Subscriptions			Х	x	
View Available Enforce Software	x	х	Х	x	
Update Enforce Software			Х	x	
NETWORKS	1			1	
View Networks	x	х	Х	x	
Create Networks			Х	х	
Edit Networks			Х	x	
Delete Networks			Х	x	

PORTS				
View Ports	х	X	х	х
Create Ports			x	x
Edit Ports			x	X
Delete Ports			х	х
POLICIES				
View Policies	х	Х	х	х
Create Policies			x	х
Edit Policy Settings			х	х
Delete Policies			x	х
SUBSCRIPTIONS		_		
View Subscriptions	X	x	x	х
Manage Subscriptions			x	х
UNEXPECTED BLOCKS		-		
Run Analysis	x	x	x	х
Add Entry to Allow List			x	х
REPORTS		_		
View Reports	x	x	x	х
View Scheduled Reports	x	x	x	Х
Schedule Reports			x	х
Edit Scheduled Reports			x	х
Delete Scheduled Reports			х	х
	MARKE	TPLACE	1	
View Products	Х	Х	x	х
View Product Details	Х	X	x	х
Subscribe to a Product				х
	MESS	AGES		
View Messages	X	X	x	Х

, p

threateg

Delete Messages	x	x	x	x
	ADMINIST	RATION		
USERS			•	
View Users	х	х	х	x
Create User				x
Edit Users			х	x
Delete Users				Х
SUBSCRIPTIONS				
View Subscriptions	х	х	х	x
COMMAND LOGS				
View Command Logs	х	х	х	х
ENFORCE DOWNLOADS				
Manual Downloads	х	х	х	x
	COMPANY	PROFILE		
Allow SSO to Create New Users				x
Allow API Access				x
Require MFA for Company				х
	IOC SE	ARCH		
Search Indicators	х	х	х	х

e.

User Management

User Management					
		View	Create	Edit	Delete
	CMP Read Only	Х	Х	Х	X
CMP Master	CMP Help Desk	Х	Х	Х	X
CIVIP Waster	CMP Admin	Х	Х	Х	X
	CMP Master	Х	Х	Х	X
	CMP Read Only	Х		Х	
	CMP Help Desk	Х		Х	
CMP Admin	CMP Admin	Х		Х	
CMP Maste	CMP Master	Х			
	CMP Read Only	Х			
	CMP Help Desk	Х			
CMP Help Desk	CMP Admin	Х			
	CMP Master	Х			
	CMP Read Only	Х			
	CMP Read Only CMP Admin	Х			
CIMP Read Only		Х			
	CMP Master	Х			