

How-To Guide

Configuring Microsoft Defender to Forward Logs to EventTracker

Publication Date:

April 4, 2022

Abstract

This guide provides instructions to retrieve the **Microsoft Defender** events via the Azure Event Hub and then configure the **Azure function app** to forward the logs to EventTracker. After EventTracker receives the logs from the Event Hub, the reports, dashboard, alerts, and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 and later and Microsoft Defender for Endpoint.

Audience

The Administrators who are assigned the task to monitor the **Microsoft Defender** events using EventTracker.



Table of Contents

Та	ble	e of C	Contents	.3
1.	(Over	view	.4
2.	I	Prere	equisites	.4
3.	(Conf	iguring Event hub to Forward Logs to EventTracker	.4
	3.1	L	Creating an Event Hubs namespace and an Event Hub	.4
	3.2	2	Configuring Azure Function app to forward data to EventTracker	.6
	3.3	3	Cost Management	15
	3.4	1	Verifying Function App	15
4.	(Conf	iguring Microsoft Defender to Forward Logs to Event hub	17
	4.1	L	Configuring Microsoft Defender to stream events to Event Hub	17
	Ab	out	Netsurion	19
	Со	ntac	t Us	19

1. Overview

Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

EventTracker helps to monitor events from the Microsoft Defender for Endpoint. Its dashboard and reports will help you track, alert information, and alert evidence which in turn help to detect file-less attacks, backdoor drops, and virus/malware.

2. Prerequisites

- An Azure Subscription and a user who is a global administrator.
- Azure Resource group.
- EventTracker Manager public IP address.
- Download Azure integration package from <u>ETS_Microsoft_Defender_Forwarder.zip</u>

3. Configuring Event hub to Forward Logs to EventTracker

Microsoft Defender can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

3.1 Creating an Event Hubs namespace and an Event Hub

The Event Hubs namespace contains one or more Event Hubs. The configured Azure services create Event Hub in these namespaces to store activities and diagnostics logs.

- 1. Login to portal.azure.com
- 2. Navigate to All services > Event Hubs > Add.

*	Dashboard > Event Hubs				
+ Create a resource	Event Hubs	\$ X			
🛧 Home	+ Add				
Dashboard	Subscriptioner Virual Studio Illimata with MSDN – Don't raa a subscription? Open Directory + Subscription rationer				
E All services	Filter by name All resource groups All locations All tags No grouping	~			
+ FAVORITES	(items				
🕅 Resource groups	NAME ↑↓ TYPE ↑↓ RESOURCE GROUP ↑↓ LOCATION ↑↓ SUBSCRIPTION ↑↓				
All resources		÷			
(L) Recent					
Virtual machines					
Subscriptions					
Monitor					
Help + support					
Advisor	No event hubs namespaces to display				
Cost Management + Billing	Try changing your filters if you don't see what you're looking for.				
Azure Active Directory	Create event hubs namespace				
PevTest Labs					
Lab Accounts					



3. Create a namespace. Provide a Namespace Name, e.g. MyEventTrackerHub, Resource group, and any other settings -> Review + Create.

Recommendation: Create and choose Resource group Name with "EventTracker". It would give a better picture of the billing for the services.

PROJECT DETAILS		
Explore the subscription to manage danlow	od resources and costs. Use resource groups like folders to organ	70 00d
manage all your resources.	ed resources and costs, use resource groups like rolders to organ	ze and
Subscription *	Azure subscription 1	~
	There supported to	
Resource group *	ETSIEM	\sim
INSTANCE DETAILS	Create new	
INSTANCE DETAILS Enter required settings for this namespace	Create new	: units.
INSTANCE DETAILS Enter required settings for this namespace Namespace name *	Create new c, including a price tier and configuring the number of throughput MyEventTrackerHub	units.
INSTANCE DETAILS Enter required settings for this namespace Namespace name *	Create new e, including a price tier and configuring the number of throughpu MyEventTrackerHub .servicebu	: units. ✓ us.windows.net
INSTANCE DETAILS Enter required settings for this namespace Namespace name * Location *	Create new c, including a price tier and configuring the number of throughpu MyEventTrackerHub .servicebu (US) West US 2	: units. ✓ us.windows.net ✓
INSTANCE DETAILS Enter required settings for this namespace Namespace name * Location * Pricing tier (View full pricing details) *	Create new c, including a price tier and configuring the number of throughpu MyEventTrackerHub .servicebu (US) West US 2 Basic (1 Consumer group, 100 Brokered connections)	: units.
INSTANCE DETAILS Enter required settings for this namespace Namespace name * Location * Pricing tier (View full pricing details) *	Create new c, including a price tier and configuring the number of throughpu MyEventTrackerHub .servicebu (US) West US 2 Basic (1 Consumer group, 100 Brokered connections)	: units.

4. On the Event Hubs namespace page, Click **Properties** under **Settings** on the left panel and copy the **Resource ID** value, Which will be used in <u>further</u> steps (4.1 step 3)

<u>∽</u>	Stream-defenderevents	Properties
-0	Event Hubs Namesnace	

Event hubs Namespace	
	«
	Name
Settings	Stream-defenderevents
📍 Shared access policies	
🔽 Scala	kesource type
Scale	Microsoft.EventHub/namespaces
Geo-Recovery	
A Encryption	Location
Encryption	Central India
🔁 Properties	
A Locks	Location ID
	centralindia
Entities	
Event Hubs	
Event hubs	/subscriptions/5ab4a53e-dff9-40ac-b1cc-e6a67f26e177/resourceGroups/az_con_gp_01/providers/Microsoft.EventHub/namespa 🗋
Monitoring	

5. On the Event Hubs namespace page, select **Event Hubs** on the left menu. At the top of the window, click **+ Event Hub**.



myehubns - Event Hubs	s				×
	K Event H	ub 🖸 Refresh			
E Overview	Search	to filter items			
Access control (IAM)	NAME	STATUS	MESSAGE	ETENTION PAR	TITION COUNT
🕐 Tags	no Event H	ubs yet.			
✗ Diagnose and solve problems					
Events					
Settings					
Shared access policies					
Geo-Recovery					
😥 Firewalls and virtual networks					
E Properties					
Locks					
🖳 Automation script					
Entities					
🗵 Event Hubs					
Monitoring					
🤑 Alerts					
Metrics					
Diagnostic settings					
1	•				•

 Type a name for your Event Hub and provide the EventHub name, partition count based on your environment, Copy the Event Hub name which will be used in <u>further</u> steps (4.1 Step 3), and then click Create.

Create Event Hub	
Name * 🛈	
EventTrackerHub	~
Partition Count ①	
0	2
Message Retention	
	1
Capture ()	
On Off	

3.2 Configuring Azure Function app to forward data to EventTracker

Azure Functions is a solution for easily running small pieces of code, or **functions**, in the cloud. For more details on the function app overview and cost, refer to the <u>link</u>.

1. Navigate to **All Services > Function App** and click the **+ Add** button.



All services > Function App	
Function App secintelkp	
$+$ Add 🔯 Manage view \vee 🖒 Refresh \downarrow Export to CSV	🖉 Assign tags
Filter by name Subscription == all Resource g	group == all 🛛 🔊
Showing 0 to 0 of 0 records.	
Name $\uparrow \downarrow$	

- 2. In the configure function app window,
 - In **Project Details**, select the desired subscription and **Resource Group**.
 - In Instance Details:
 - Provide a function app name, like FunctionEventTracker.
 - Select Code in Publish option.
 - In Runtime stack, select PowerShell Core.
 - Select the appropriate **region.**

Recommendation: Create and choose Resource group Name with "EventTracker". It would give a better picture of the billing for the services.

Create Function App

Create a function app, which lets you group functions as a logical unit for easier management, deployment and sharing of resources. Functions lets you execute your code in a serverless environment without having to first create a VM or publish a web application.

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subserieties *		
	PAYG-ET-AZORE-RP-DEV	~
Resource Group * ①	az_con_gp_01	\sim
	Create new	
Instance Details		
Function App name *	FunctionEventTracker	✓
		.azurewebsites.net
Publish *	● Code ○ Docker Container	
Runtime stack *	PowerShell Core	\sim
Version *	7.0	
version "	7.0	~
Region *	Central US	\sim
Review + create < Previou	us Next : Hosting >	

- 3. Click Next: Hosting.
 - Under Storage Section, select your storage account.
 - Under the Operating system, select Windows.
 - Under Plan, choose a plan of your choice.



All services > Function App >	Function App	
Function App		
Basics Hosting Moni	toring Tags Review + create	
Storage		
When creating a function app, Queue, and Table storage.	you must create or link to a general-purpose Azure Storage account tha	t supports Blobs,
Storage account *	(New) storageaccountetsie9304	\sim
	Create new	
Windows is the only supported Operating System *	I Operating System for your selection of runtime stack.	
Plan		
The plan you choose dictates h	now your app scales, what features are enabled, and how it is priced. Lea	rn more 🖾
Plan type * 🕕	Consumption (Serverless)	\sim
- •	· · ·	
Review + create	< Previous Next : Monitoring >	

- 4. Click **Review + Create**.
- 5. After the **Function** app is created, navigate to All services > Function App > FunctionEventTracker to do further configuration and click on Advanced **tools** under **Development** Tools.

FunctionEventTracker Functions						
	🕂 Create 🖒 Refresh 🛛 🔟 Delete					
Development Tools						
Sector Console						
下 Advanced Tools	_					
✓ App Service Editor (Preview)	Name ↑↓					
Extensions	EventHubTrigger1					

6. Click **Go** and provide Azure credentials.

- C		
ELS	U	®

FunctionEventT	rack	er Advanced Tools …
✓ Search (Ctrl+/)	«	<u> </u>
Development Tools	•	Advanced Tools
≥. Console		Advanced Tools provides a collection of dev
K Advanced Tools		Go →
App Service Editor (Preview)		
Extensions		

7. A new browser window opens. Select **PowerShell** from **Debug console** menu.

Kudu Env	vironment Debug console -	Process explorer	Tools -	Site extensions
/ + 4 it	cmb PowerShell			

 Click on + and click on New folder provide a folder name such as ETS_Microsoft_Defender_FunctionApp.



9. Click on folder which was created on last step



10. Copy the Base path as shown below, which will be used in the future step (step 21)

(Example path: - C:\home\ETS_Microsoft_Defender_FunctionApp)



... / ETS_Microsoft_Defender_FunctionApp +

Name



11. Drag and drop the **Support** folder (as received in the integration package) to create a folder. A new **Support** folder is added.

/ ETS_Microsoft_Defender_FunctionApp		
	Name	
ŦO	🖀 Support	

12. Navigate to the **Support/** folder and click on the **Edit** button for the **Details.xml** file.

/ Sup	port 🛨 🛛 4 items 🖌 🏠 💄
	Name
±/O	Data Encryption.dll
±₽0	Details.xml
1/0	EtsIns.dll
1/0	EvtTrkList.dll

13. Here,

- In line number 9, mgr_name, provide the EventTracker Manager hostname.
- In line no. 10, **mgr_port**, enter the EventTracker Manager port number, e.g., 14505.
- In line number 11, mgr_ip, provide the EventTracker Manager public IP address.
- In line number 13, **org_name**, provide your organization name and org_name can only contain A-Z, a-z, 0-9, and Under score(_).



1	<objs <="" th="" version="1.1.0.1"></objs>
2	<pre>mlns="http://schemas.microsoft.com/powershell/2004/04"></pre>
3	白 <obj refid="0"></obj>
4	<pre><tn refid="0"></tn></pre>
5	<t>System.Management.Automation.PSCustomObject</t>
6	<t>System.Object</t>
7	-
8	白 < <u>MS></u>
9	<s n="mgr_name">ET.CONTOSO.LOCAL <!-- Replace with EventTracker manager name. e.g., ET.CONTOSO.LOCAL--></s>
10	S N="mgr_port">14505 Replace with EventTracker manager port. e.g., 14505
11	<pre><s n="mgr_IP">198.17.23.198</s> <!-- Replace with EventTracker manager public IP address. e.g., 198.17.23.198--></pre>
12	<pre><s n="sys_ip">127.0.0.1</s></pre>
13	<s n="org_name">EventTracker <!-- Replace with Organization Name. e.g., EventTracker--></s>
14	-
15	
16	- 0bj
17	L

- 14. Click Save.
- 15. Come back to the Function APP tab (navigate to All services > Function App > FunctionEventTracker) to do further configuration and click **Functions** under Functions.



16. Click Create.

{fx} FunctionEventTracker Functions … Function App			
✓ Search (Ctrl+/) «	🗧 🕂 Create 🖒 Refresh 🛛 🕅 Delete		
🤣 Overview			
Activity log	✓ Filter by name		
Access control (IAM)	Name 1		
Diagnose and solve problems	No results.		
🏮 Security			
🗲 Events (preview)			
Functions			
{ f x} Functions			
📍 App keys			
🛷 App files			
A Drovies			

17. Select the Develop in portal option and click the Azure Event Hub trigger.

Netstrion

 \times

 \times

Create function

Select development environment Instructions will vary based on your development environment. Learn more			
Development environ 🕀 De	velop in portal		
Select a template			
Use a template to create a function. Trigg	gers describe the type of events that invoke your functions. Learn more		
√ Filter			
Azure Service Bus Queue trigger	A function that will be run whenever a message is added to a specified Service Bus queue		
Azure Service Bus Topic trigger	A function that will be run whenever a message is added to the specified Service Bus topic		
Azure Blob Storage trigger	A function that will be run whenever a blob is added to a specified container		
Azure Event Hub trigger	A function that will be run whenever an event hub receives a new event		
Azure Cosmos DB trigger	A function that will be run whenever documents change in a document collection		
IoT Hub (Event Hub)	A function that will be run whenever an IoT Hub receives a new event from IoT Hub (Event Hub)		
SendGrid	A function that sends a confirmation e-mail when a new item is added to a particular queue		
Azure Event Grid trigger	A function that will be run whenever an event grid receives a new event		
Durable Functions HTTP starter	A function that will trigger whenever it receives an HTTP request to execute an orchestrator function $lacksim v$		
•	•		
Create Cancel			

18. In the Event Hub connection, click **New**.

Create function

Azure Service Bus Topic trigger	A function that will be run whenever a message is added to the specified Service Bus topic
Azure Blob Storage trigger	A function that will be run whenever a blob is added to a specified container
Azure Event Hub trigger	A function that will be run whenever an event hub receives a new event
Azure Cosmos DB trigger	A function that will be run whenever documents change in a document collection
IoT Hub (Event Hub)	A function that will be run whenever an IoT Hub receives a new event from IoT Hub (Event Hub)
SendGrid	A function that sends a confirmation e-mail when a new item is added to a particular queue
Azure Event Grid trigger	A function that will be run whenever an event grid receives a new event
Durable Functions HTTP starter	A function that will trigger whenever it receives an HTTP request to execute an orchestrator function \downarrow
•	

Template details

We need more information to create the Azure Event Hub trigger function. Learn more

New Function *	EventHubTrigger1
Event Hub connection * ①	No existing connections available \checkmark
	New
Event Hub name* $^{\odot}$	samples-workitems
Event Hub consumer group 🛈	\$Default
Create Cancel	



19. Let Azure populate the available Event Hub namespace and Event Hub. Select the desired ones and click **Ok.**



20. Click Create.

Create function

 \times

Azure Service Bus Topic trigger	A function that will be run whenever a message is added to the specified Service Bus topic
Azure Blob Storage trigger	A function that will be run whenever a blob is added to a specified container
Azure Event Hub trigger	A function that will be run whenever an event hub receives a new event
Azure Cosmos DB trigger	A function that will be run whenever documents change in a document collection
IoT Hub (Event Hub)	A function that will be run whenever an IoT Hub receives a new event from IoT Hub (Event Hub)
SendGrid	A function that sends a confirmation e-mail when a new item is added to a particular queue
Azure Event Grid trigger	A function that will be run whenever an event grid receives a new event
Durable Functions HTTP starter	A function that will trigger whenever it receives an HTTP request to execute an orchestrator function \checkmark
▲	•

Template details

We need more information to create the Azure Event Hub trigger function. Learn more

New Function *	EventHubTrigger1
Event Hub connection*①	hubaks_RootManageSharedAccessK \vee
	New
Event Hub name*①	samples-workitems
Event Hub consumer group ①	\$Default
Create Cancel	

21. Click **Code+Test** and copy the contents of **ETS_Microsoft_Defender_forwarder.ps1** (as received in the integration package) and paste it into the given **run.ps1** window in the Azure function app portal and replace the path which was copied on **step 10** (Example path: - C:\home\ETS_Azure_FunctionApp) and click **Save.**

EventHubTrigger1 Code + Test				
✓ Search (Ctrl+/)	« 🗟 Save 🗙 Discard 🖒 Refresh 🖽 Test/Run 주 Upload			
[fs] Overview	testing1603 \ EventHubTrigger1 \ run.ps1 \			
Developer 1 <# · -=>ETS Microsoft Defender · Forwarder · <=======				
Code + Test	2 Dille Maren - A FTC Minner ff Defender Serverder ant			
Integration	4 ····Version ·····: 1.0			
Monitor	5 ····Created······: 28-03-2022 6 ····Author······: Harish·C·M, Netsurion Technologies PVT.·LTD. ("EventTrackerâ€圆)			
📍 Function Keys	7 ····Purpose·····: This script will help to forward Microsoft Defender for Endpoint logs from Event hub to EventTracker.			
	9 #>			
	10 param(\$eventHubMessages, \$TriggerMetadata)			
	11 Spath =: "C:\home\ETS_Microsoft_Defender_Forwarder" #Replace *path folder with the Base path where you have uploaded Support folder the base of the proceedable is a contract.			
	12 - **triecks if the base path is exist 13 - *:f(Test-path Spath)			

3.3 Cost Management

- The below-mentioned services are charged by Microsoft based on usage.
 - Function App
 - Click here Function-App-price-tier to know more on pricing details.
 - Event Hub Click here Event-Hub-price-tier to know more on pricing details.

3.4 Verifying Function App

- Once the Function App is deployed, follow the below-mentioned steps to verify the deployment.
 - 1. Login to https://portal.azure.com/
 - 2. Search for Function App service.
 - 3. Click on created Function App.
 - 4. On successful deployment the screen would look as shown below.



• Sometimes due to the mismatch of the extension package one could see below-mentioned error. Below are the steps provided to remediate the issue.

🗹 Browse	🕐 Refresh	Start	C Restart	\rightleftarrows Swap	🞍 Get publish profi	e 7	Reset publish profile	$\overline{\uparrow}$	Download app content	Ŵ	Delete	🔗 Senc
Microso Extensic version	ft.Azure.WebJol onStartupType E of 4.3.0.0. Upda	bs.Script: On ventHubsWe te your NuG	e or more load bJobsStartup fi et package refe	ed extensions rom assembly erence for Mic	do not meet the minimi 'Microsoft.Azure.WebJo rosoft.Azure.WebJobs.Ex	im requi os.Eventi tensions	rements. For more inforr Hubs, Version=4.1.1.0, Cu EventHubs to 4.3.0 or la	mation ulture ter.	n see https://aka.ms/func-n =neutral, PublicKeyToken=	nin-ex 31bf3	ktension-v 856ad364	versions. 4e35' does



- To check the extension bundle.
 - 1. Click on **App files** under the Function section in the left pane of the function App home page
 - 2. Choose host.json from the dropdown
 - 3. Modify the version details in the JSON file to "version": "[2.*, 3.0.0)"
 - 4. Click Save.

Function App	
,P Search (Ctrl+/)	« 🗟 Save × Discard 🕐 Refresh
Functions	
[6] Functions	testv400 \ host.json \
📍 App keys	1
App files	3 "managedDependency": {
Proxies	4 ···· "Enabled": true 5 ··},
Deployment	6 "extensionBundle": { 7 "id": "Microsoft Azure Functions.ExtensionBundle",
😇 Deployment slots	8 "version": "[2.*, -3.0.0)"
Deployment Center	10)

- \circ ~ To check the Function App run time version.
 - 1. Click on **Configuration** under Settings in the left pane of the function App home page.
 - 2. Click on Function runtime settings.
 - 3. Choose Runtime version to ~3 from the dropdown.
 - 4. Click Save.

Function App				
✓ Search (Ctrl+/)	~	🟷 Refresh 🛛 🗟 Save	e 🗙 Discard 🗢 Leave Fee	edback
Settings	•	Application settings	Function runtime settings	General settings
Authentication		Runtime version		
Application Insights		~1	\sim	
🚷 Identity		~1		
🔗 Backups		0		
😾 Custom domains		 When the daily usa 	ge quota is exceeded, the funct	tion app is stopped un
TLS/SSL settings				

• Click on the **Overview** in the left pane to go to the **Function App** home page.

Now the home page should not be showing the earlier error message as shown below.



P Search (Ctrl+/) ≪	🗹 Browse 💍 Refresh 🔲 Stop 📿 Restar	t $~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~$	content ····
🦘 Overview	Click here to access Application Insights for moni	toring and profiling for your app. \rightarrow	
Activity log	↑ Essentials		JSON View
Access control (IAM)	Resource group (move)	UBI	
Tags	az con gp 01	https://xyz321.azurewebsites.net	
Diagnose and solve problems	Status Running	Operating System Windows	
Security	Location	App Service Plan	
🗲 Events (preview)	Central India	ASP-azcongp01-9c11 (Y1: 0)	
Functions	Subscription (<u>move</u>) PAYG-ET-AZURE-KP-DEV	Properties See More	
[fi] Functions	Subscription ID 5ab4a53e-dff9-40ac-b1cc-e6a67f26e177	Runtime version 3.4.2.0	
📍 App keys	Tags (edit)		
App files	Click here to add tags		

4. Configuring Microsoft Defender to Forward Logs to Event hub

Microsoft Defender for Endpoint can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

4.1 Configuring Microsoft Defender to stream events to Event Hub

Login to <u>security.microsoft.com</u> using the admin account and <u>create an event hub namespace</u>, if not created.

1. Click on Settings on the left panel and click Microsoft 365 Defender.



2. Click Streaming API and Click on +Add.

Settings 🗧 Microsoft 365 Defender

Streaming API

Account	Configure direct export of events from Microsoft 365 Defender to Azure Available Capacity 4/5			
Email notifications				
Preview features	+ Add			
Streaming API	Name	Event Hub Resource Group		

3. Configure Stream API.



- Fill Name like EventTracker.
- Check the box Forward event to Azure Storage.
- **Paste** Event-Hub Resource ID (Copied on 3.1 step 4).
- **Paste** Event-Hub name (Copied on 3.1 step 6).
- Check the box Alerts under Events Types.
- Click Submit.

Add new Streaming API settings

Configure new Streaming API settings, in order to forward Microsoft 365 Defender events to Azure storage and / or event hub. Read about how to fill this form

Name * EventTracker	
Forward events to Azure Storage	
Forward events to Event Hub	
Event-Hub Resource ID *	_
/subscriptions/5ab4a53e-dff9-40ac-b1cc-e6a67f26e177/resourceGroups/az_con_g	
Event-Hub name ①	
MicrosoftDefender	
Events Types (2/20)	
V Alerts	Q
	Ģ
Submit Cancel	

4. After successful configuration the following screen display.

Settings > Microsoft 365 Defender

Streaming API

Account	Configure direct export of events from M Available Capacity 3/5	icrosoft 365 Defender to Azure
Email notifications		
Preview features	+ Add	
Streaming API	Name	Event Hub Resource Group
	EventTracker	az_con_gp_01



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion <u>Managed Threat Protection</u> combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion <u>Secure Edge Networking</u> delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>.

Contact Us Corporate Headquarters

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2) EventTracker Enterprise for MSPs SOC: 877-333-1433 (Option 3) EventTracker Essentials SOC: 877-333-1433 (Option 4) EventTracker Software Support: 877-333-1433 (Option 5) https://www.netsurion.com/eventtracker-support