

Integration Guide

Integrating Cisco[®] Secure Endpoint with EventTracker

Publication Date:

May 17, 2022

Abstract

This guide provides instructions to retrieve the **Cisco® Secure Endpoint** events via remote syslog. Once the logs start coming into EventTracker, then reports, dashboards, alerts, and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and **Cisco®** Secure Endpoint.

Audience

Administrators who are assigned the task to monitor the **Cisco® Secure Endpoint** events using EventTracker.



Table of Contents

| Tab | le of (| Contents |
|-----|---------|---|
| 1. | Ove | rview4 |
| 2. | Prer | equisites4 |
| 3. | Integ | gration of Cisco [®] Secure Endpoint events to EventTracker4 |
| 4. | Ever | ntTracker Knowledge Packs8 |
| 4 | .1 | Category |
| 4 | .2 | Alerts |
| 4 | .3 | Reports |
| 5. | Impo | orting Cisco [®] Secure Endpoint Knowledge Pack into EventTracker8 |
| 5 | .1 | Category9 |
| 5 | .2 | Alerts |
| 5 | .3 | Knowledge Objects (KOs)11 |
| 5 | .4 | Reports |
| 6. | Veri | fying Cisco [®] Secure Endpoint Knowledge Pack in EventTracker14 |
| 6 | .1 | Category14 |
| 6 | .2 | Alerts |
| 6 | .3 | Knowledge Objects15 |
| 6 | .4 | Report16 |
| Д | bout | Netsurion |
| C | ontac | rt Us17 |

1. Overview

Cisco[®] Secure Endpoint (formerly AMP for Endpoints) integrates prevention, detection, threat hunting, and response capabilities in a single solution, leveraging the power of cloud-based analytics. Secure Endpoint will protect your Windows, Mac, Linux, Android, and iOS devices through public or private cloud deployment.

EventTracker helps to monitor events from Cisco[®] Secure Endpoint. Its knowledge objects and flex reports will help you to analyse scanning details, threat detection and quarantine details, vulnerable application details, as well as suspicious and system activities.

2. Prerequisites

- EventTracker v9.x or above should be installed.
- A user with global administrator access of Cisco[®] Secure Endpoint.
- Administrative access on EventTracker.

3. Integration of Cisco[®] Secure Endpoint events to EventTracker

To configure the Cisco[®] Secure Endpoint integration.

Generating Client ID and API Key:

- 1. Log into https://console.amp.cisco.com/ (N.A.) or https://console.eu.amp.cisco.com/ (E.U.)
- 2. Go to the Business Page from the Accounts dropdown menu.
- 3. Click the **Edit** button.
- 4. Under features, click the **Regenerate** button beside **3rd Party API Access** to generate the **Client ID** and **secure API Key**
- 5. Once you have the API client ID and API key, you can get the logs as follows:

| The API credenti | als have been generated. Keep the new API credentials in a password manager or encrypted file |
|------------------|---|
| 3rd Party AP | I Client ID |
| | 538 |
| API Key | |
| | 21996 |

Following are the steps to integrate Cisco Secure Endpoint into EventTracker.

- 1. Get the Cisco[®] Secure Endpoint executable file: <u>https://downloads.eventtracker.com/kp-integrator/ETS_Cisco Secure Endpoint_Integrator.exe</u>
- 2. Once the executable application is received, click the file ETS_Cisco Secure Endpoint_Configure.

| ETS Cisco Secure Endpoint Integrator |
|---|
| Help |
| Client ID: |
| API Key: |
| Organization Name: |
| Validate Credentials Edit |
| EventTracker Configuration Use EventTracker Agent Configuration |
| Manager: |
| Manager Port: Test Connection |
| |
| Finish Cancel |

3. **Cisco[®] Secure Endpoint Integrator** window is displayed. Fill in the **Client ID**, and **API Key** as received from the web interface of Cisco[®] Secure Endpoint, and provide the **Organization Name**.

| Clien | t ID: e | | |
|--------------------|-------------------------|-------------------|----|
| API | Key: e0. | | |
| Organization Na | ame: ETS | | |
| | Validate Credentials | Edit | |
| EventTracker Confi | guration | | |
| | Use EventTracker Age | ent Configuration | |
| N | lanager: | | _ |
| Manag | ger Port: | Connecti | or |
| | | | _ |



4. Once you have filled out the fields, click the **Validate** button to check if the credentials are correct and working properly.



 If the Agent is installed on the server where the program is launching, the EventTracker Agent Configuration check box is enabled to use the Agent machine etaconfig.ini file manager details to send the logs.

| | | - 2 | |
|----------------------------|--------------------|------------------|--------------------|
| Client ID: e | | | |
| API Key: e0. | | | |
| Organization Name: ETS | | | |
| Va Cre | lidate dentials | Edit | |
| EventTracker Configuration | | | |
| ✓ Use Eve | ntTracker Age | nt Configuration | ı |
| Manager: | | | 24.5 |
| Manager Port: | | ÷ | Test Connection |
| | | | |
| | | | |

6. If the user wants to send the logs to specific EventTracker, then the user needs to mention EventTracker Manager IP and Manager Port to send the logs and click Test Connection to check the connectivity.

| Help | to secure Endpoint integrator |
|----------|--|
| | Client ID: |
| | API Key Classic mente or policionous |
| 0 | FTS |
| Orgi | anization Name. |
| | Validate Edit |
| _ | |
| Eventir | acker Configuration |
| | Manager: 172.28.9.67 |
| | Manager Port 14505 |
| | Connection |
| | |
| | Finish |
| | Curres |
| ormation | |
| | |
| | |
| | ntegrator is connected with EventTracker manager successfully. |
| | |
| | |
| | |

7. Once everything verified, click the **Finish** button to complete the Integration.



8. Run ETS_Cisco Secure Endpoint_LogForwarder exe to get the logs into EventTracker.

4. EventTracker Knowledge Packs

After the logs are received by the EventTracker Manager, Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs (KPs) are available in EventTracker to support Cisco[®] Secure Endpoint.

4.1 Category

• **Cisco**[®] **Secure Endpoint** - **Events** - This category provides information about all the events such as scan details, Threat Detected and Quarantine Details, Vulnerable Application and Fault Detected, Suspicious Activity Detected, System Activity, File activity.

4.2 Alerts

• **Cisco**[°] **Secure Endpoint – Risk Detected** – This alert generates when any risk is detected for the event_type_id like 1091567628, 1090519054, 1005, 1090524040 etc.

4.3 Reports

• **Cisco**[°] **Secure Endpoint – Events** – This report gives information about all the events which are generated from Cisco[°] Secure Endpoint.

5. Importing Cisco[®] Secure Endpoint Knowledge Pack into EventTracker

NOTE: Import Knowledge Pack items in the following sequence:

- Category
- Alerts
- Knowledge Objects
- Reports
- Dashboards
- 1. Launch EventTracker Control Panel.
- 2. Double click **Export Import Utility**.

Netstrion®

| 8 | Even | tTracker Contro | I Panel | _ 🗆 🗙 |
|-----------------------------|-----------------------|-------------------|-----------------------|-------------|
| | | NE | Ev | entTracker |
| EventVault | Diagnostics | License | Export Import | Append |
| 00 | | Manager | | Archives |
| EventTracker Agent Confi | Traffic Analyzer | Agent Manageme | Port Configuration | TrapTracker |
| Change Audit | About EventTracker | | | |
| | E-mail: s | support@EventTra | cker.com | |

3. Click the **Import** tab.

5.1 Category

1. Click the **Category** option, and then click the browse button.

| 9 | Export Import Utility | – 🗆 X |
|--|---|--------------|
| Export Import | | |
| 1. Provide the path and file name 2. Click the Import button. | e of the Categories file. Use the '' button to browse and locate the import file. | |
| Options | Location | |
| Category | | |
| Filters | | |
| ⊖ Alerts | | |
| Systems and Groups | Source : | |
| O Token Value | | |
| O Reports | | |
| Behavior Correlation | | |
| | | |
| | | |
| L | Imoot | Close |
| | import | CIUSE |

- 2. Locate the Categories_Cisco Secure Endpoint.iscat file, and then click the Open button.
- 3. To import categories, click the **Import** button.

EventTracker displays a success message.



4. Click **OK**, and then click the **Close** button.

5.2 Alerts

1. Click the **Alerts** option, and then click the **browse** button.

| B | Export Ir | nport Utility | _ | | c | | |
|---|---|---|--------------------------|-------|---|--|--|
| Export Import | | | | | | | |
| 1. Provide the path and file nam 2. Click the Import button. | on to browse and locate the import file. | | | | | | |
| Options | Location | | | | | | |
| Category | Cat Astive | | | | | | |
| ⊖ Filters | Only if notifications set | This setting is applicable only for imports from Alert files. For v 7, the active status will be set | Legacy (v6x) based on | | | | |
| Alerts | By default | "Active" key available in the configuration se | ction. | | | | |
| O Systems and Groups | Watchlist Configuration | | | | | | |
| O Token Value | ✓ Import Watchlist configuration | | | | | | |
| | This setting is applicable only for alerts which have Advanced watchlist configured. Note: If this option is enabled the user should make sure the watchlist groups are available. | | | | | | |
| Reports | on the console where the alert | s are imported. | | | | | |
| O Behavior Correlation | | | | | | | |
| | Source : | | | _ | | | |
| | *.isalt | | | | | | |
| | | | _ | | | | |
| | | | | | | | |
| | | Law 2 | | 0 | 5 | | |
| | | Impo | JTL | Liose | | | |

- 2. Locate the Alerts_Cisco Secure Endpoint.isalt file, and then click the Open button.
- 3. To import alerts, click the **Import** button. EventTracker displays a success message.



4. Click **OK**, and then click **Close**.

5.3 Knowledge Objects (KOs)

1. Click Knowledge Objects under the Admin option in the EventTracker Manager page.

| ≡ | EventTracker | | | | | .▲ Admin• | Tools - |
|----------|--|---|---------------------------------|-------------------|---------------------------|------------------------|--------------------|
| | Home | | Active Watch Lists | Collection Master | Group Management | Systems | 🕈 / Dashb |
| ٥ | | | Alerts | Correlation | 🔍 IP Lookup Configuration | QQ Users | |
| | 0 | 1 | Behavior Correlation Rules | Diagnostics | 🔅 Knowledge Objects | 🕀 Weights | |
| ~ | | | 🇞 Behavior Correlation Settings | Event Filters | Manager | 🔲 Windows Agent Config | |
| | Potential Cyber Breaches Unsafe connections or processes, new TCP entry point | Indicators of Cc USB activities, New sen | Casebook Configuration | 🔮 Eventvault | 🧭 Parsing Rules | | |
| | | | | FAQ Configuration | Report Settings | | |
| | Attacker | | | - News | | | |

2. Click the **Import** U button as highlighted in the below image:

| | Knowledge Obj | 🕈 / Admin / Knowledge Object | .5 | | | |
|--------|----------------|------------------------------|----|--------------|-----------------|---|
| Q K | Search objects | Q | Q | Activate Now | Objects 🕀 📳 🏦 🛱 | 1 |
| | Groups | 0 🖉 🗊 | | | 1 1 | |
| | | | | | | |
| | EventTracker | | | | | |

3. Click Browse.



- 4. Locate the file named **KO_Cisco Secure Endpoint.etko**.
- 5. Select the check box and then click the \square Import option.

| Impor | t | | × |
|-------|-----------------------|-----------------------|-----------------------|
| Sele | ct file | | The Browse Upload |
| | Object name | Applies to | Group name |
| | Cisco Secure Endpoint | Cisco Secure Endpoint | Cisco Secure Endpoint |

6. Knowledge Objects are now imported successfully.

| File imported successfully. | |
|-----------------------------|--|
| ОК | |

5.4 Reports

1. Click the **Reports** option and select the **New (*.etcrx)** option.

| Provide the path and file nam Click the Import button Note : if report(s) contains temp Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation | ne of Schedule Report file. Use the '' button to browse and locate the import file. Iate, first import template and proceed with exportimport utility. Location Legacy (*issch) Source : *issch |
|---|--|
|---|--|

2. Locate the file named Reports_Cisco Secure Endpoint.etrcx and select all the check box.

| Frequency Show all Q Q Title Sites Groups Systems Frequence Extint Sites Groups Systems Undefined | Image: Secure Endpoint - Events | Frequency Show all Sites | - Q Q Groups | Systems | Frequency |
|--|--|--|----------------------------------|---------|-----------|
| Thie Sites Groups Systems Frequence ED11 Csco Secure Endpoint - Events Undefined Undefined e: Set run time option is not applicable for Defined Reports and Hourly Reports et at interval of minutes Set Set t run time for report(s) from AM • at interval of minutes Set Option Set Option | The The EDIT Cisco Secure Endpoint - Events | Sites | Groups | Systems | Frequency |
| Image: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM * at interval of | EDIT Cisco Secure Endpoint - Events | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM v at interval of minutes Set ① | | | | | Undefined |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM ~ at interval of minutes Set place to Replace Are in partners | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM ~ at interval of minutes Set ① place to Replace Are protected. | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set place to | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set ① | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set place to | | | | | |
| 2 Set run time option is not applicable for Defined Reports and Hourly Reports run time for report(s) from AM 		 at interval of minutes Set ① lace to Replace Again systems | | | | | |
| tet run time option is not applicable for Defined Reports and Hourly Reports n time for report(s) from AM 		 at interval of minutes Set ① ce to Replace Assimptions | | | | | |
| Set run time option is not applicable for Defined Reports and Hourly Reports in time for report(s) from AM - at interval of minutes Set ① Ce to Replace Assign extreme | | | | | |
| Set run time option is not applicable for Defined Reports and Hourly Reports in time for report(s) from AM • at interval of minutes Set ① CR to Replace Assimptions | | | | | |
| Set run time option is not applicable for Defined Reports and Hourly Reports un time for report(s) from AM v at interval of minutes Set ① acc to Replace Assim partements | | | | | |
| s: Set run time option is not applicable for Defined Reports and Hourly Reports run time for report(s) from AM • at interval of minutes Set 1 | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports run time for report(s) from AM • at interval of minutes Set ① alace Replace Assim sustains | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set 1 | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set ① | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set place to Replace Arsign systems | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set ① | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set ① | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set 10 Diage Replace Arsign systems | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports : run time for report(s) from AM • at interval of minutes Set ① | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports : run time for report(s) from AM • at interval of minutes Set 1 | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports : run time for report(s) from AM • at interval of minutes Set ① | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports run time for report(s) from AM • at interval of minutes Set 1 | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports run time for report(s) from AM • at interval of minutes Set ① | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports run time for report(s) from AM • at interval of minutes Set place to Replace Assign systems | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports run time for report(s) from AM • at interval of minutes Set ① | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports run time for report(s) from AM • at interval of minutes Set place to Resigner systems | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports run time for report(s) from AM • at interval of minutes Set vlace to | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports run time for report(s) from AM • at interval of minutes Set place to | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set place to | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM < at interval of minutes Set Diace to | | | | | |
| e: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set | | | | | |
| t run time for report(s) from AM • at interval of minutes Set | | | | | |
| t run time for report(s) from AM • at interval of minutes Set () | te: Set run time ontion is not applicable for Define | 1 Reports and Hourly Reports | | | |
| | te: Set run time option is not applicable for Define | d Reports and Hourly Reports | | | |
| | te: Set run time option is not applicable for Define | d Reports and Hourly Reports | | | |
| place to Penlace Assistence | te: Set run time option is not applicable for Define | d Reports and Hourly Reports | set () | | |
| place to Benlace Assim systems | te: Set run time option is not applicable for Define t run time for report(s) from | d Reports and Hourly Reports | es Set | | |
| place to Replace Assign systems | e: Set run time option is not applicable for Define t run time for report(s) from | d Reports and Hourly Reports AM • at interval of minute | es Set | | |
| Tiopidoo 7-baigit systema | e: Set run time option is not applicable for Define t run time for report(s) from | d Reports and Hourly Reports | es Set | | |
| | e: Set run time option is not applicable for Define t run time for report(s) from place to | d Reports and Hourly Reports AM at interval of Repl Repl | es Set () lace Assign systems | | |

3. Click the **Import** I button to import the report. EventTracker displays a success message.



6. Verifying Cisco[®] Secure Endpoint Knowledge Pack in EventTracker

6.1 Category

- 1. Log on to **EventTracker**.
- 2. Click the Admin dropdown, and then click Category.

| ≡ | Event Tracker ⊕ | | | | | Admin• | Tools - |
|---|--|---|---------------------------------|-------------------|---------------------------|----------------------|--------------------|
| | Home | | Active Watch Lists | Collection Master | Group Management | Systems | 🕈 / Dasht |
| a | | | Alerts | Correlation | 🔍 IP Lookup Configuration | 🙊 Users | |
| | 0 | 1 | Behavior Correlation Rules | Diagnostics | · Knowledge Objects | 1 Weights | |
| ~ | | Indicators of Cc USB activities, New sen | 🗞 Behavior Correlation Settings | ⊽ Event Filters | Manager | Windows Agent Config | |
| | Potential Cyber Breaches Unsafe connections or processes, new TCP entry point | | Casebook Configuration | Eventvault | 🧭 Parsing Rules | | |
| | | | 📲 Category | FAQ Configuration | Report Settings | | |
| | Attacker | | - News | | | | |

3. In the **Category Tree** to view the imported category, scroll down and expand the **Cisco**[®] **Secure Endpoint** group folder to view the imported category.



6.2 Alerts

- 1. Log on to **EventTracker**.
- 2. Click the **Admin** menu, and then click **Alerts**.

| ≡ | Event Tracker ⊕ | | | | | 🔎 Admin- | Tools - |
|----------|--|-------------------------|---------------------------------|--------------------------|---------------------------|----------------------|--------------------|
| | Home | | Active Watch Lists | Collection Master | Group Management | Systems | 🕈 / Dashl |
| Q | | | ▲ Alerts | C Correlation | 🔍 IP Lookup Configuration | 🙊 Users | |
| | 0 | 2 | Behavior Correlation Rules | Diagnostics | · Knowledge Objects | T Weights | |
| <u>~</u> | | | 🇞 Behavior Correlation Settings | Event Filters | Manager | Windows Agent Config | |
| | Potential Cyber Breaches Unsafe connections or processes, new TCP entry point | USB activities, New sen | Casebook Configuration | Eventvault | 🧭 Parsing Rules | | |
| | | | oe Category | FAQ Configuration | Report Settings | | |
| | Attacker | | | News | | | |

3. In the **Search** box, type **Cisco[®] Secure Endpoint**, and then click the **Go** button. The Alert Management page will display the imported alert.

| ÷ | Activate Now | Click 'Activate Now' after making all changes |
|---|--|---|
| | | Alert Name 🔨 |
| | ត្រុង Cisco Secure Endpoint: Risk det | ected |
| | | |

4. To activate the imported alert, toggle the **Active** switch.

EventTracker displays a message box.



5. Click **OK**, and then click the **Activate Now** button.

NOTE: Specify the appropriate **system** in **alert configuration** for better performance.

6.3 Knowledge Objects

1. In the EventTracker web interface, click the Admin dropdown, and then select Knowledge Objects.

| = | Event Tracker ⊕ | | | | | Admin- | Tools - |
|---|--|---|---------------------------------|-------------------|---------------------------|----------------------|--------------------|
| | Home | | Active Watch Lists | Collection Master | Group Management | Systems | 🕈 / Dashb |
| a | | | Alerts | C Correlation | 🔍 IP Lookup Configuration | 🛱 Users | |
| | 0 | 1 | Behavior Correlation Rules | Diagnostics | · Knowledge Objects | T Weights | |
| | | | 🗞 Behavior Correlation Settings | Event Filters | @ Manager | Windows Agent Config | |
| | Potential Cyber Breaches Unsafe connections or processes, new TCP entry point | Indicators of Cc USB activities, New sen | Casebook Configuration | 🔮 Eventvault | 🧭 Parsing Rules | | |
| | | | o-[o Category | FAQ Configuration | Report Settings | | |
| | Attacker | | | - News | | | |

2. In the Knowledge Object tree, expand the **Cisco**[®] **Secure Endpoint group** folder to view the imported knowledge object.



| Knowledge Objects | | | | | | |
|-----------------------|------------|---|---|--|--|--|
| Search objects | | Q | Q | | | |
| Groups | 🕀 🧭 i | Î | | | | |
| Cisco Secure Endpoint | | | | | | |
| Cisco Secure Endpoint | Ø 1 | Ì | | | | |

3. Click Activate Now to apply imported knowledge objects.

6.4 Report

1. In the **EventTracker** web interface, click the **Reports** menu, and then select **Report Configuration**.

| | Event Tracker ⊕ | | | |
|---|------------------------|------------|--|---|
| | Home | | | |
| ۹ | | 1 | 1 | |
| R | Report Configuration | | | |
| | Report Dashboard | ntry point | Indicators of Compromise USB activities, New services or software install | |
| | Explorer | | | |
| | Attacker | I | | - |

- 2. In **Reports Configuration** pane, select the **Defined** option.
- 3. Click the **Cisco[®] Secure Endpoint** group folder to view the imported reports.

| Rep | orts configu | ration: Cisco Secure Endpoint | | | | | |
|-----|--------------|--------------------------------|--------------------|--------------------|----|---|----------|
| ÷ | Ū | | | | | T | 'otal: 1 |
| | | Title | Created on | Modified on | | | |
| | £3 | Cisco Secure Endpoint - Events | Apr 13 02:44:55 AM | May 11 11:41:00 PM | () | 5 | + |
| | | | | | | | |
| | | | | | | | |

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's <u>EventTracker</u> cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for 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>. Netsurion is #23 among <u>MSSP Alert's 2021 Top 250 MSSPs</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 MSP's 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