CISCO
SECURE

At a Glance
Cisco Public

Cisco Secure Network Analytics Endpoint License

The Cisco Secure Network Analytics Endpoint license allows you to conduct in-depth, context-rich investigations into endpoints that exhibit suspicious behavior.

A lot of things have fundamentally changed how users work today. Applications, data, and user identities have moved to the cloud, branch offices connect directly to the internet, and many users work off-premises, which has given them an unprecedented ability to access, create, and share information online. This has naturally had the side effect of increasing the likelihood of them exposing sensitive information.

Security professionals need comprehensive visibility into all user and endpoint behavior both on and off premise. The Secure Network Analytics (formerly Stealthwatch) solution provides security analysts the information they need to conduct more efficient and context-rich investigations into user machines that exhibit suspicious behavior. Tightly integrated with the Cisco AnyConnect Network Visibility Module (NVM), the Cisco Secure Network Analytics Endpoint License extends network visibility to provide insights into user behavior, applications, and processes running on remote devices to speed up incident response times and policy violation remediations.

Benefits

- **Increased visibility:** Extends your network as a sensor to personal devices such as laptops, tablets, and smart phones.
- **Enhanced security:** Delivers enhanced security with real-time threat detection on suspicious activity and potential attacks.
- **Accelerated response:** Provides superior forensic investigations with sophisticated security analytics.
- **Improved compliance:** Offers real-time situational awareness and network visibility to help you meet compliance regulations across your entire network.

CISCO The bridge to possible

Components

In addition to the Cisco Secure Network Analytcis Endpoint license you will also need the following components.

Network Visibility Module: The Network Visibility Module (NVM) generates rich flow context data from endpoints both on and off premise. This telemetry is sent to the Flow Collector and then the Cisco Secure Network Analytics solution to provide visibility and analytics into network connected devices and user behaviors.

Endpoint License: The Endpoint License allows telemetry data to be exported from endpoint devices on your network. The license permits the high-value endpoint contextual data provided by the Cisco AnyConnect NVM to be exported to the Endpoint Concentrator: for further analysis by Secure Network Analytics. The number of endpoint licenses should be equal to the number of deployed Cisco AnyConnect NVM licenses.

Endpoint Concentrator: The Endpoint Concentrator is a virtual appliance that collects nvzFlow data from the Cisco AnyConnect NVM. Data is collected from all endpoint devices and is passed through the Endpoint

How It Works

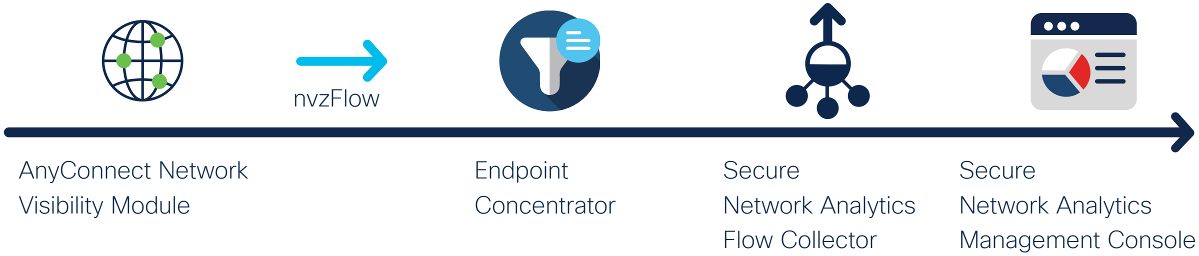
The Endpoint License supports the Cisco® Network Visibility Flow (nvzFlow) protocol, an extension of the IP Flow Information Export (IPFIX) protocol, that collects standard flows from endpoints as lightweight standard IPFIX records.

The Cisco AnyConnect NVM gathers high-value endpoint contextual data and leverages the nvzFlow protocol to export that telemetry to the Endpoint Concentrator. The Endpoint Concentrator collects this telemetry from multiple endpoints and forwards it to the Flow Collector.

There, through a process of stitching and deduplication, the endpoint-specific fields are inserted into the conversational flow records maintained in the Flow Collector database. The endpoint data is then analyzed and displayed in the Csico Secure Network Analytics management console for a single view into activity across the network..

Generating this telemetry and context is a critical step towards gaining the visibility needed to secure the endpoint.

Figure 1. Cisco Secure Network Analytics Endpoint Solution Architecture


nvzFlow
AnyConnect Network Visibility Module
Endpoint Concentrator
Secure Network Analytics Flow Collector
Secure Network Analytics Management Console

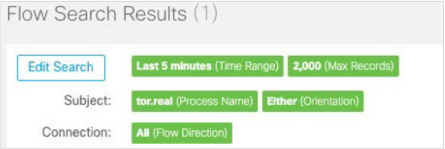
Components and Architecture

Figure 1 illustrates the components and architecture of this solution.

Flow search on enhanced endpoint telemetry

Leverage endpoint details to identify:

- Unwanted applications
- Security evasion and attribution
- Assets used by applications
- Day-Zero malware and perform threat hunting

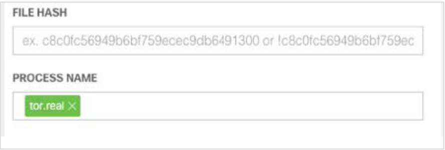


Flow Search Results (1)

Edit Search | **Last 5 minutes** (Time Range) | **2,000** (Max Records)

Subject: **tor.real** (Process Name) | **Either** (Orientation)

Connection: **All** (Flow Direction)

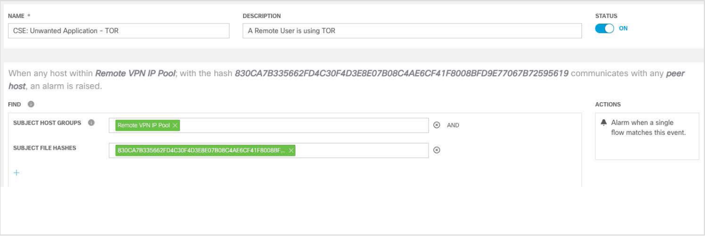


FILE HASH: ex. c8c0fc56949b6bf759ecec9db6491300 or !c8c0fc56949b6bf759ec

PROCESS NAME: tor.real ✕

Use endpoint details to guide your security policies

Create security events for when remote users violate corporate policies and investigate and respond to detected occurrences.



NAME *: CSE: Unwanted Application - TOR

DESCRIPTION: A Remote User is using TOR

STATUS: ON

When any host within ***Remote VPN IP Pool***; with the hash ***830CA7B335662FD4C30F4D3E8E07B08C4AE6CF41F8008BFD9E77067B72595619*** communicates with any ***peer host***, an alarm is raised.

FIND

SUBJECT HOST GROUPS: Remote VPN IP Pool ✕ AND

SUBJECT FILE HASHES: 830CA7B335662FD4C30F4D3E8E07B08C4AE6CF41F8008BF... ✕

ACTIONS: Alarm when a single flow matches this event.

Take the next steps

Learn more about Cisco Secure Network Analytics

Check out the Cisco Secure Network Analytics Datasheet

Try Secure Network Analytics today with a free Visbility Assessment

Read the Deployment Guide to learn more about how the Cisco Secure Network Analytics Endpoint License would work in your environment