

Cisco Endpoint Security Analytics (CESA) Built on Splunk POV Kit Lab

Last Updated: 05-MAR-2021

Product Overview:

Cisco Endpoint Security Analytics (CESA) and AnyConnect Network Visibility Module (NVM) enables deep endpoint visibility by using IPFIX endpoint telemetry to identify flow traffic and provide attributes such as source address, source port, destination address, destination port, process name, destination host and other valuable attributes to identify insider and behavioral-based threats such as application/SaaS abuse, endpoint security evasion, zero-trust abuse, data loss detection and day-zero malware and threat hunting. CESA complements other endpoint security, such as EPP and EDR, by detecting unknown malware and behavioral-based threats that are outside the purview of endpoint anti-malware platforms.

Cisco AnyConnect Network Visibility Module (NVM) is configurable feature set included in Cisco AnyConnect ver. 4.2 or later. Cisco NVM produces customized IPFIX endpoint telemetry information when the device is either on or off the network. This data is collected by CESA built on Splunk, where it is ingested and becomes readily available as Splunk events and Cisco Splunk NVM Dashboards and panels in CESA.

CESA analyzes endpoint telemetry generated by the Network Visibility Module (NVM) built into the Cisco AnyConnect Secure Mobility Client. CESA Built on Splunk is Splunk Enterprise software that is tuned and priced per endpoint to analyze NVM telemetry produced by endpoints to detect a variety of endpoint-specific security risks and breaches, such as:

- Finding unapproved or blacklisted SaaS and client applications
- Discovering day-zero malware and conduct threat hunting
- Identifying endpoints trying to evade security scanning or disable client-side security software
- Monitoring pertinent activity and behavior of endpoints when they are not attached to the network, such as in zero-trust deployments
- Analyzing data and traffic types going across VPN tunnels and split tunnels
- Deep behavioral monitoring of remote endpoints
- Creating endpoint software application and process whitelists
- Detecting data theft and data loss
- Performing endpoint asset inventory or OS's, user accounts, device manufacturers/model and software under IT management on the network

CESA Built on Splunk is sized on a per-endpoint basis for 1 and 3 year terms that can be deployed as: 1) a standalone AnyConnect NVM analytics platform or, 2) may be combined with an existing Splunk deployment as a feature license to add per-endpoint priced analytics specifically for AnyConnect NVM telemetry. In this feature license scenario,

AnyConnect NVM telemetry does not count against the data volume license used on the broader Splunk deployment, but is instead counted on a per-endpoint basis based on the capacity of the CESA Built on Splunk endpoint capacity purchased.

About This Lab

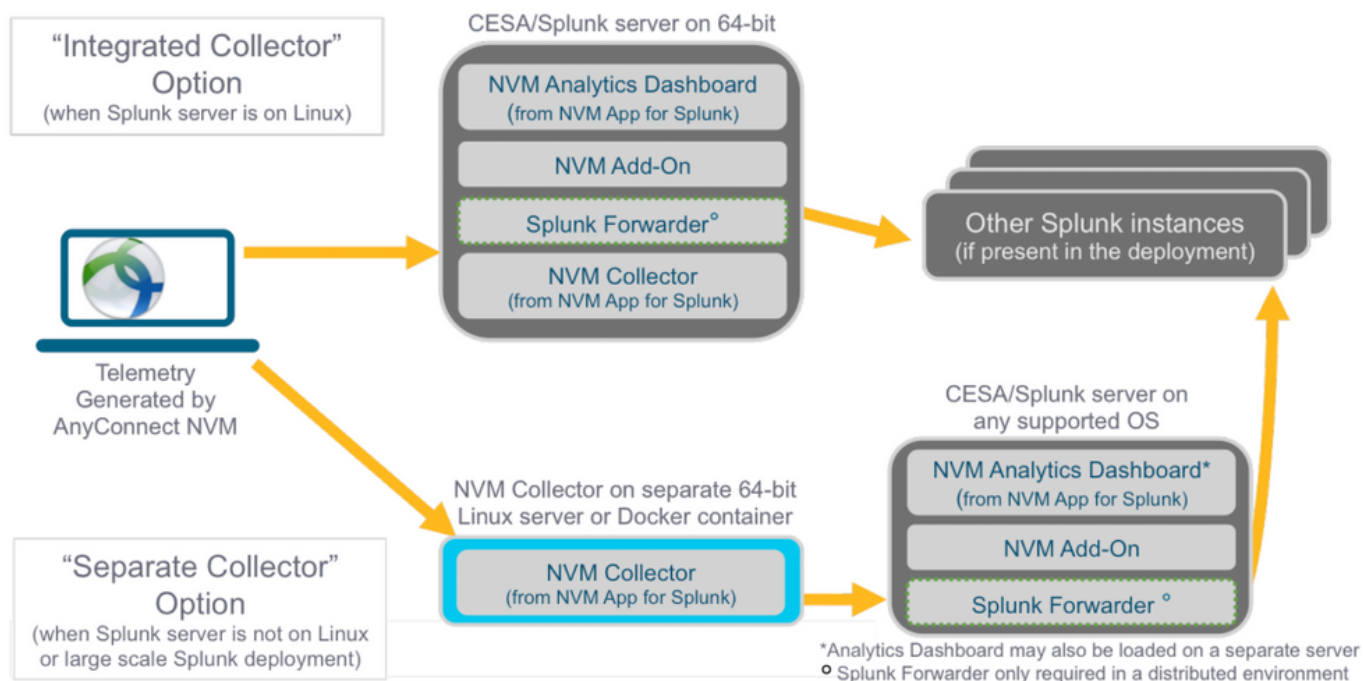
This lab will allow you to quickly learn how to work with the CESA “10-Minute” POV Kit. A self-contained kit to get you up and running quickly (designed to be installable in an existing Splunk environment in 10 minutes or less) to showcase data to show the value of what Splunk and CESA have to offer. There are other components setup in the Cyber Defense Clinic Lab we are using to run this training lab that won't be utilized. You will be using the Windows JumpHost only during the lab. This lab will help you understand the deployment architecture of CESA Built on Splunk, how to download, load the apps and work with the POV kit data.

This lab will not go into the following but is covered in the [community guide](#):

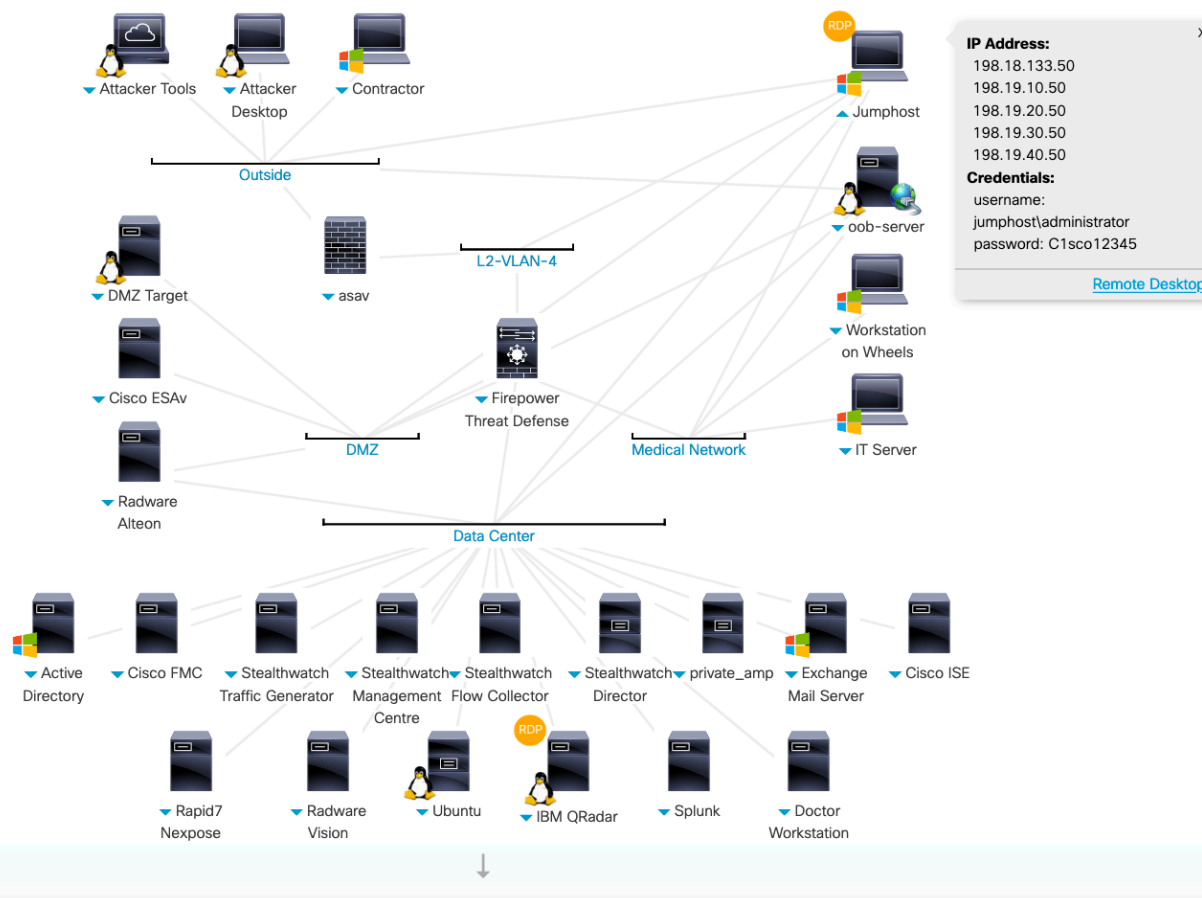
- Licensing
- Support
- Setup of AnyConnect NVM or Splunk

This lab was built off the cs.co/cesa-pov community document that is the ultimate source of truth and latest information for the POV kit. It also utilizes the below Cisco dCloud lab topology in a limited capacity. Its built off the [Cyber Defense Clinic Lab](#). You can schedule this if you'd like on your own as an employee or partner, even share with your customer.

CESA Deployment Architecture Options



Cyber Defense Clinic Lab Topology



In the lab you will want to copy/paste from your local desktop to your dCloud setup

You can copy/paste utilizing Guacamole from your local machine to the WKST in dCloud by:

1. copying local desktop
2. initiating the command (this will show a window)
 - a. On MAC – CTRL + SHIFT + Command
 - b. On windows – CTRL + ALT + SHIFT
3. pasting into that window
4. toggling the window again
5. pasting using Windows Remote

You will need to have an account with Splunk to download the needed applications.

Step 1. Create an account with Splunk

This lab requires you to have a login to <http://splunkbase.splunk.com/>. If you already have an account then skip to Step 2.

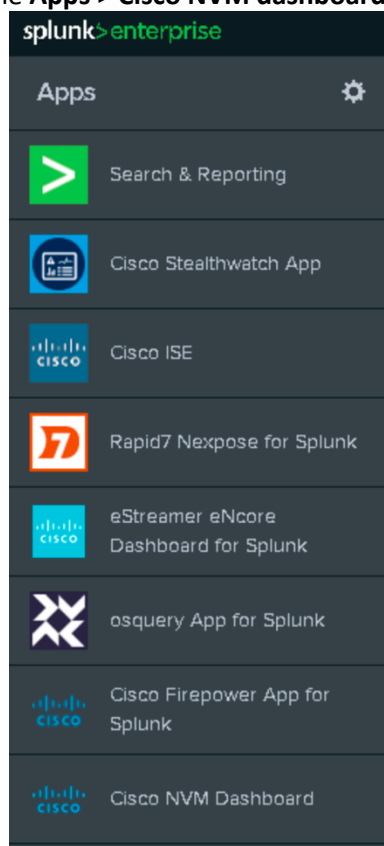
1. Go to **My Account > Signup**
2. Create an account
3. Make sure you use your partner email address (example: **@partner.com**) email, and partner name to make sure it doesn't lock out due to export restrictions.
4. You will have to validate this email
5. You should have an account quickly. If not ask the proctor or a classmate to login for you.

Step 2. Connect to the JumpBox dCloud and Login to Splunk

This is the only device you will be using in this lab. All the other devices are for other deliveries.

From your session **topology view** click on the **AD Server** to access the remote desktop

1. Use the **JumpServer** to access to **Splunk Enterprise**.
2. Use the bookmark in Chrome to access Splunk.
3. Login with **admin/C1sco12345**
4. Once logged into Splunk access the **Apps > Cisco NVM dashboard**



Step 3. Download, install (update) and become familiar with the 2 apps

For this lab using the Cyber Defense Clinic you can simply update the apps in Splunk console. If you're using these steps on a system without them then you can use the information at <http://cs.co/cesa-pov> to get the download information from Splunkbase.

Here we will login to Splunk and update in the UI (older systems might need to have the user download and do a manual install)

1. In the upper left **Click the gear next to Apps**
2. Sort the list by **name**.
Notice if any of them need **updates** there will be a link next to them.
3. Click the **Update to 2.x.x**, it will ask you to login with your Splunk account to do the update. The below example has an older version but same concept.
The 2 apps with possible updates and are needed in this setup are:
Cisco NVM Add-on for Splunk & Cisco NVM Dashboard

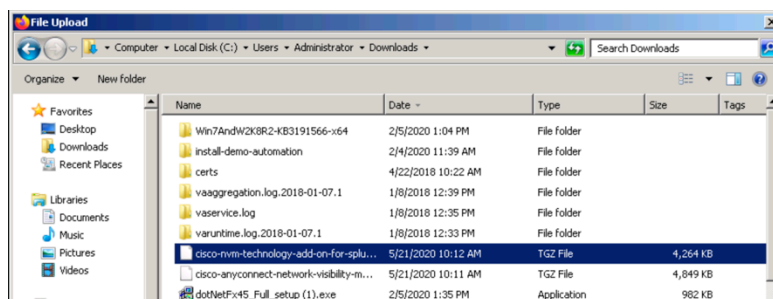
Name	Folder name	Version
Apps Browser	appsbrowser	8.0.1
Cisco AMP for Endpoints Events Input	amp4e_events_input	11.7
Cisco Firepower App for Splunk	firepower_dashboard	1.3.7
Cisco ISE	Splunk_CiscoISE	2.0.6
Cisco NVM Add-on for Splunk	TA-Cisco-NVM	2.1.2
Cisco NVM Dashboard	CiscoNVM	2.0.187 Update to 2.1.2

If you are missing the ability to update from the UI then please install updates manually

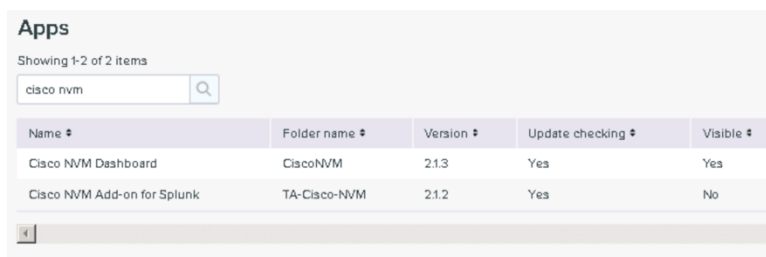
1. On the jump host navigate to <http://splunkbase.splunk.com> and login with your personal account
2. Search for **cisco nvm**
3. *There are 2 apps, download them both*

4. Next go to **manage apps** on Splunk UI and in the **upper right install app from file**

- a. Browse to C:/users/administrator/downloads
- b. Sort by date and details and you will see the 2 files downloaded



- c. Make sure to upgrade the app after choosing each of them to install



These have been recently updated as of May 2020 with new use cases please always check <http://cs.co/cesa-pov> for any changes

Here we explain the 2 components and how they are used in an actual live deployment. These won't require any customization when doing a POV using the CESA POV Kit. This is just for your information.

Cisco Endpoint Analytics Built on Splunk: CESA is the NVM-customized Splunk Enterprise platform that performs security analytics on AnyConnect NVM telemetry produced by endpoints. In addition to the base Splunk Enterprise software included in CESA, there are two NVM-specific components:

Cisco AnyConnect Network Visibility Module (NVM) App for Splunk - use v2.1.x or later

- 1) Serves as a “collector” for NVM flows coming from endpoints; this collector component may be installed directly on a Splunk forwarder in the CESA Built on Splunk instance or on a separate Linux-based server. For demo environments the solution can also be run on a single 64-bit Linux system that includes both the NVM collector and Splunk Enterprise components for demonstration purposes.
- 2) Provides pre-designed analytics dashboards to visualize, view and set alerts on the data. This component enables immediate visibility into endpoints and user activities, but can also be endlessly customized or even completely replaced with a custom developed deployment-specific CESA console using standard Splunk query and visualization capabilities.

Cisco NVM Technology Add-On for Splunk - use v2.1.x or later

This “technology add-on” (aka “TA” in Splunk nomenclature) provides NVM data indexing and formatting inside CESA Built on Splunk. It takes NVM data from the endpoint “collector” noted above in the AnyConnect NVM App for Splunk and translates the NVM flow data into syslog that can be processed and analyzed by CESA Built on Splunk. Like any Splunk TA, it is installed within the Splunk Enterprise instance of CESA Built on Splunk.

Step 4. Download the POV Kit, clear out old data, and install the data.

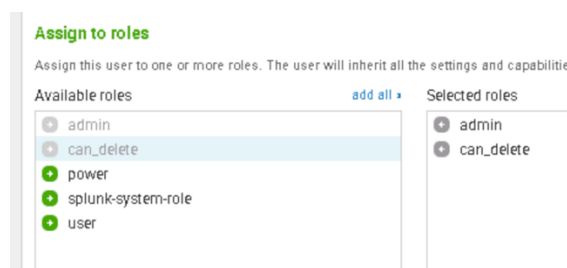
1. Download the zip file and extract.

- On the **Remote Desktop** and your local machine. Download the CESA POV Kit attached to near the bottom of the <http://cs.co/cesa-pov>.
- Find the download and **extract the files**. You can delete the video from AD downloads folder on remote workstation. On your local machine you can keep everything except the video to watch the install process for the files.

2. Clear out old data

The PoV kit will be periodically updated, it is best to delete any prior data imported for these sourcetypes from an older PoV kit. You will need to give the account access to delete.

- Go to **Settings > User and Authentication > Access and Controls > select Admin**
- Next '**Assign roles**' add '**can_delete**' to your account. Click **Save** at the **bottom** of the page.



- In the **upper left**, select **App: Search and Reporting**
- In the global search, select a time range (far right) and then run the following command for each **sourcetype**.


In the CDC dCloud lab, any data for the **year-to-date** should be removed to make a clean system. In your lab or other environments you can use these settings as well since **All Time** might not be accessible option. It is disabled in this setup.

Enter **search data (listed below)**, select **time year-to-date**, and then click the **search** magnifying glass. Do this for each data file for a total of 3 deletions to make sure you got it all.

Note: the amount of records could be different. Give it a few minutes to run on flow data as it's the largest:

```
sourcetype="cisco:nvm:flowdata" | delete
sourcetype="cisco:nvm:ifdata" | delete
sourcetype="cisco:nvm:sysdata" | delete
```

New Search Save As Close

sourcetype="cisco:nv:flowdata" | delete Previous year 

✓ 54 events (1/1/19 12:00:00.000 AM to 1/1/20 12:00:00.000 AM) No Event Sampling Job || → ↓ Verbose Mode

Events (54) Patterns **Statistics (2)** Visualization

100 Per Page Format Preview

splunk_server	index	deleted	errors
splunk.ad.hacknds.com	<u>__ALL__</u>	261776	0
splunk.ad.hacknds.com	main	261776	0

New Search Save As Close

sourcetype="cisco:nv:ifdata" | delete Year to date 

✓ 5 events (1/1/20 12:00:00.000 AM to 4/25/20 9:13:44.000 AM) No Event Sampling Job || → ↓ Verbose Mode

Events (5) Patterns **Statistics (2)** Visualization

100 Per Page Format Preview

splunk_server	index	deleted	errors
splunk.ad.hacknds.com	<u>__ALL__</u>	182	0
splunk.ad.hacknds.com	main	182	0

New Search

sourcetype="cisco:nv:sysdata" | delete Job ||

✓ 3 events (1/1/19 12:00:00.000 AM to 1/1/20 12:00:00.000 AM) No Event Sampling

Events (3) Patterns **Statistics (2)** Visualization

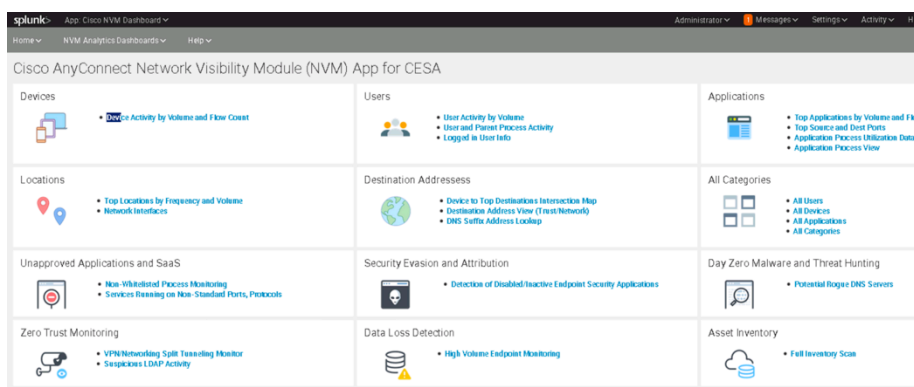
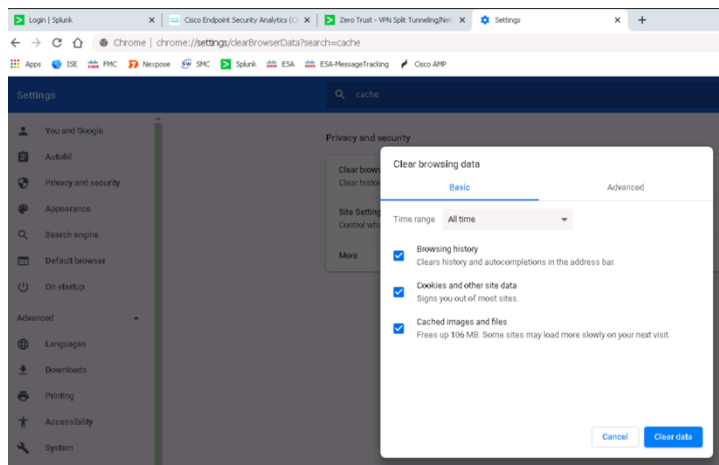
100 Per Page Format Preview

splunk_server	index	deleted
splunk.ad.hacknds.com	<u>__ALL__</u>	26
splunk.ad.hacknds.com	main	26

3. Flush out the browser cache

This is important to see the new App dashboard in case there were changes in javascript.

- Depending on the browser you're using. In this lab we are using Chrome
- Click on the **3 dots in the upper right**
- click **Settings**, search for **Cache** and **clear browsing data ALL time**

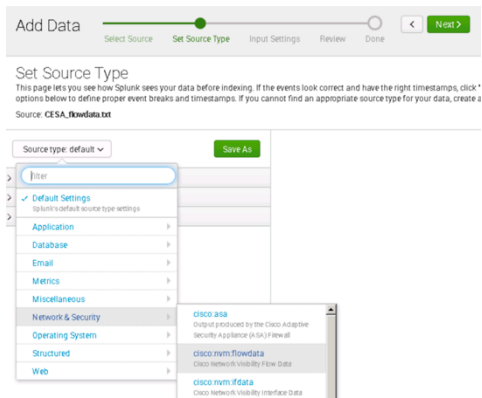


4. Import the new data

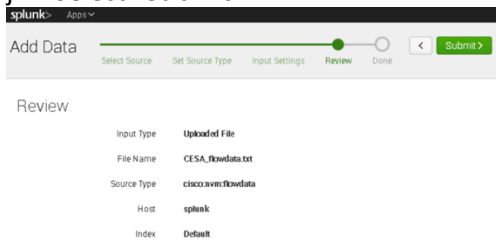
It is important that each file imported into Splunk is mapped to the appropriate sourcetype. The searches and dashboards depend on this step.

- CESA_ifdata.txt maps to sourcetype cisco:nvm:ifdata
- CESA_flowdata.txt maps to sourcetype cisco:nvm:flowdata
- CESA_sysdata.txt maps to sourcetype cisco:nvm:sysdata

- a. Select **Settings > Add Data**
- b. Select **“Upload files from My Computer”**
- c. Find the extracted files under Downloads/CESA POV Kit
- d. Select **“CESA_flowdata.txt”** File
- e. Select **Next**
- f. Now Select the **Source Type**, by default we will see “default”
- g. Select the Drop Down Icon and go to **Network & Security** and Select **“cisco:nvm:flowdata” (OR TYPE flowdata)**



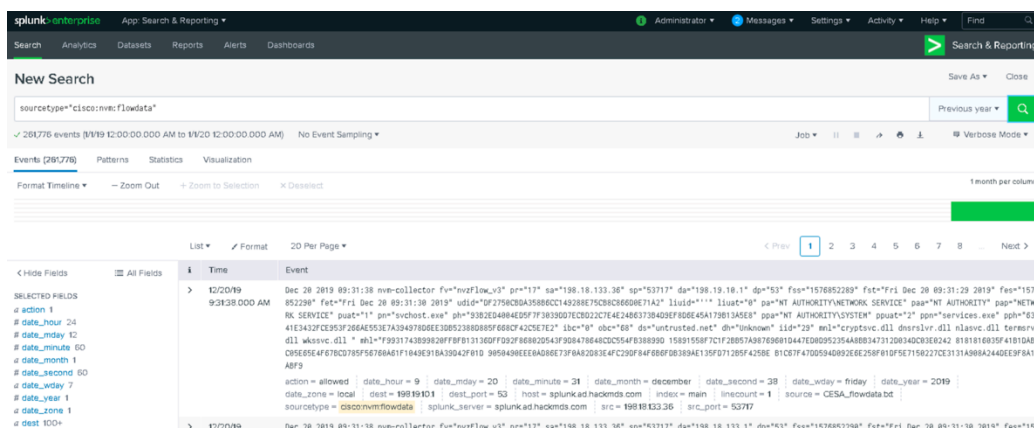
- h. Select **Next**
- i. Select **Review**
- j. Select **"Submit"**



- k. Select **Add More Data**
- l. Repeat the steps above for **ifdata.txt** (choosing sourcetype="cisco:nvm:ifdata" for mapping)
- m. Repeat the steps above for **sysdata.txt** (choosing sourcetype="cisco:nvm:sysdata" for mapping)

5. Validate the installed data

- a. Navigate to **Global Search - Upper left App: Search & Reporting**
- b. Select **previous year** on the right side
- c. Enter **sourcetype="cisco:nvm:flowdata"**
- d. Do the same for ifdata & sysdata



Getting Familiar with Network Visibility Module (NVM) Analytics Dashboard

Sample Demo Use Cases

Use Case	CESA Screen
Unapproved Applications & SaaS	Non-Whitelisted Process Monitoring Destination Address View
Security Evasion	Detection of Disabled/Inactive Endpoint Security
Day-Zero Malware & Threat Hunting	User Activity by Volume User and Parent Process Activity
Zero-Trust Monitoring	VPN/Networking Split Tunneling Monitoring
Data Loss Detection	High Volume Endpoint Monitoring
Asset Inventory	Full Inventory Scan

We are using the slide above as a guide to go over the different options available. However, we have grouped them in a different order on priority, they will not flow as seen above.

Keep in mind as you go throughout these examples you can create alerts to notify you if anything is triggered in the future. For example if hosts stop reporting on their anti-malware, if traffic to certain sites is triggered, or if certain processes communicating to wrong hosts. There are many flexible options to secure your system. This is a very powerful solution able to see everything happening across all your endpoints running AnyConnect NVM with processes, applications, DNS servers, large volume and much more.

If you wait around a little during queries you will see more data populate.

Learning to Demo CESA with Network Visibility Module Analytics Dashboard

In this lab you will learn how to demonstrate some portion of each of the major CESA use listed in the graphic above. Note that this lab doesn't cover all the capabilities of CESA for each of these use cases, but will enable you to demo examples in each use case area. Furthermore, CESA is infinitely customizable, so each of the underlying queries and alerting for these demos can be customized by any experienced Splunk customer to tailor fit their environment and needs.

Much of what you will do in this lab is demonstrate examples of how CESA uses analytics to accomplish each use case. In a customer deployment environment one would typically create automated alerts associated with these analytics so that detection of these threats becomes automated via event alerting.

Start with looking at the NVM Analytics Dashboards

In the upper left, Select **Apps** > Select **Cisco NVM Dashboard** and Select **NVM Analytics Dashboards**

When the app first starts there will be a setup screen. For the lab we will not be modifying or using any of the options. You don't need to worry about changing anything on this page. Click Save at the bottom right.

Use Case 1: Zero-Trust Monitoring : VPN/Networking Split Tunneling Monitoring

Question: How can I monitor the zero-trust traffic that is going off-net thru the split tunnel? How can I be sure sensitive traffic isn't going over the split tunnel? How can I figure out if I have other traffic I can safely put over a split tunnel? What is putting a heavy traffic load on the tunnel?

One of the top use cases right now with the current health situation around the world is the ability to check what is happening with your remote access users. This is a crucial use case. Not only does it help you analyze what traffic should be sent through the tunnel or not depending on the security sensitivity of the traffic but it also helps you analyze which traffic is heavy and doesn't need to be going through the tunnel. Example video, file sharing, conferencing and more! Some of these are Netflix, Box, WebEx.

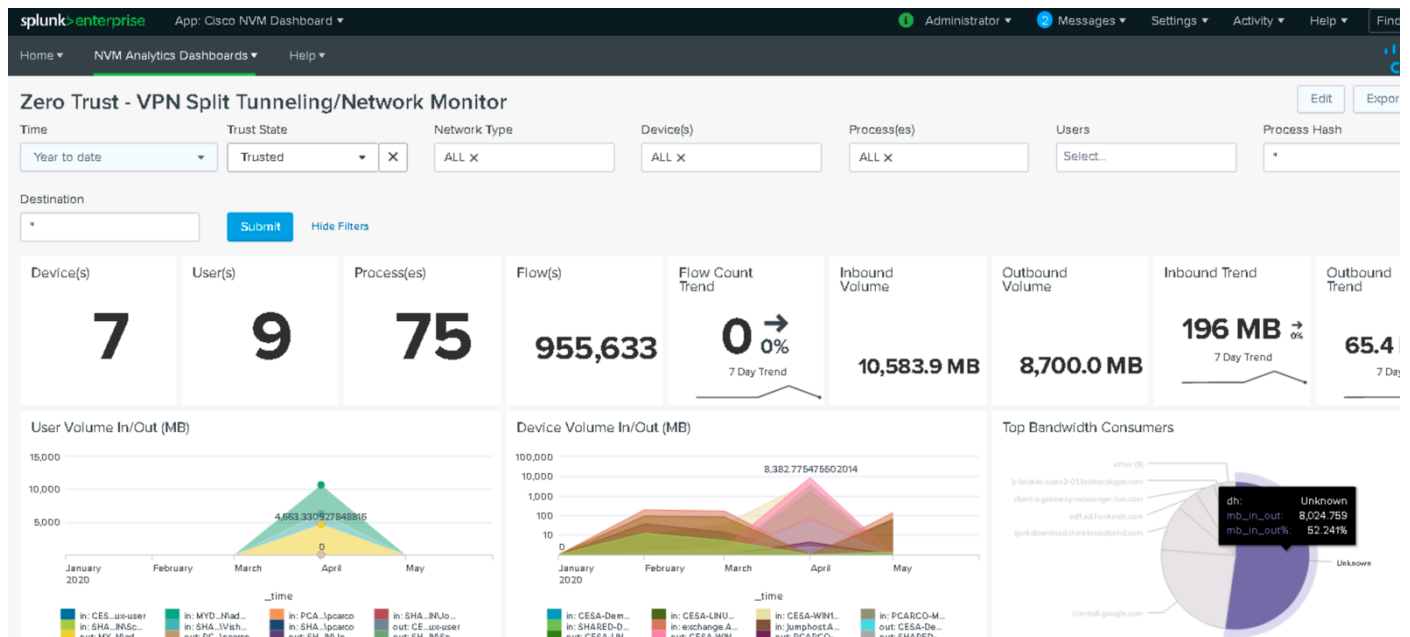
It will help customers identify the traffic and better tune their networks to send heavy traffic outside of the tunnel if its deemed not sensitive in nature. This will save the bandwidth inside the company for better performance and possible cost savings. Also it can help customers identify how they should implement split traffic if they aren't already.

1. Return to the Cisco NVM Dashboard
2. In the bottom left, Select **Zero Trust – VPN Split Tunneling/Network Monitor**
Note: By Default we will not see any events in the Dashboard because the data could be over 7 days old (simulated data)
3. In the upper left change Time **last 30 days**
4. Select **Trust State: Trusted**
5. Click **Apply** and then **Submit**

Automating this use case: These sorts of searches can be saved and made into an alert so that CESA will automatically detect these events and automatically raise an alert to the Splunk event console. Such automation is customizable for whatever data/event is important to the customer.

In this example we don't have access to show something that is heavily utilizing the tunnel like Office 365, Box, or Netflix that could be tuned to go outside of the tunnel. However you can see the type traffic selected as an example. You can customize to showcase high bandwidth or approved apps that shouldn't be going thru the tunnel

Here you can see on the Trusted side that Unknown is the highest amount. Something to investigate?



After clicking on the unit you can dig deeper into the query and investigate more

Check for Untrusted app running on Untrusted interface

Another nice example would be to check if a specific app is running. In this example we will be looking at **sshd.exe** running on the **Untrusted side** as that's not allowed. You can look at the bottom of the page and see what devices are being used. In this environment you can see a Linux machine.



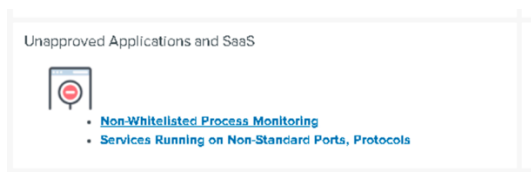
USE CASE 2a: Unapproved Applications & SaaS Non-Whitelisted Process Monitoring

Question: What apps are in use that I don't know about? What apps are there in my environment I don't want people using?

Using the unapproved applications it will showcase all traffic from applications that aren't on the companies approved application whitelist.

1. In the bottom left, Select **Non-Whitelisted Process Monitoring**

Note: By Default we will not see any events in the Dashboard because the data is over 7 days old (simulated data)

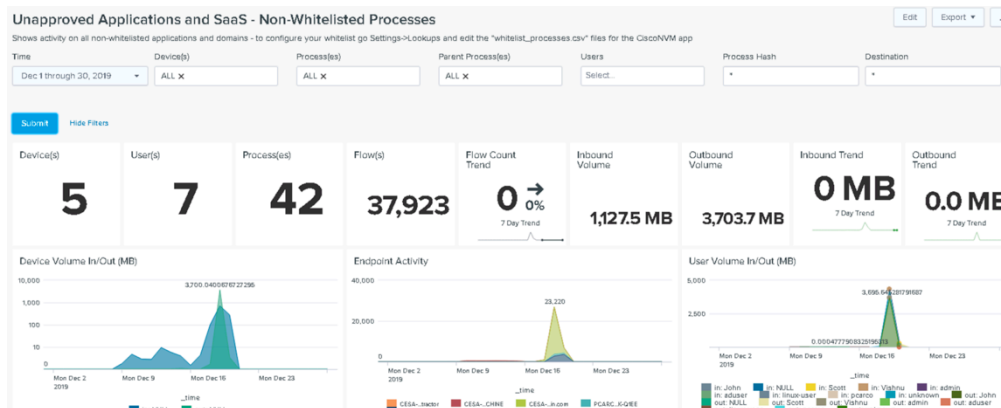


2. In the upper left change Time to **Preset – Last 30 days**, we are updating the dataset on a monthly basis

Note: we will need to use this same time concept whenever working with any of the POV dataset. This may change so please check the POV kit community page <http://cs.co/cesa-pov> in the future.

3. Click **Apply** and then **Submit**

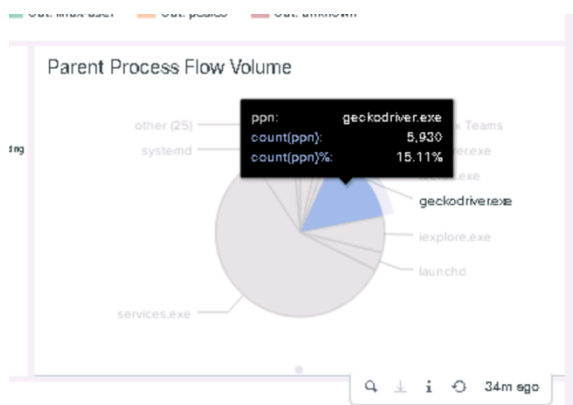
4. You will now see data per the timeset.



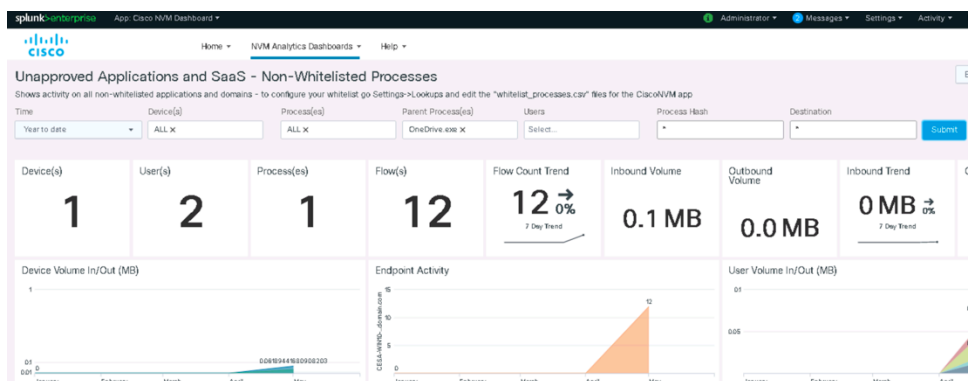
5. Let's drill down into some of that data.

What processes are going to what destinations? For example maybe you want to see what's going to "doubleclick" domain. All unauthorized applications, where are they going, what kind of data is going out? Whitelisted processes are something that is set and customizable in a CSV file that's in Splunk but not something we are going to use in this lab. Here is the hash and query on those applications. The app comes baked with a template list but that customer can adjust this to their security posture. For example what are the processes are out there. Show me everything out there and start making your own whitelist. Customers will have their own list and create their own list from Splunk and its queries. This is beyond the scope of the POV.

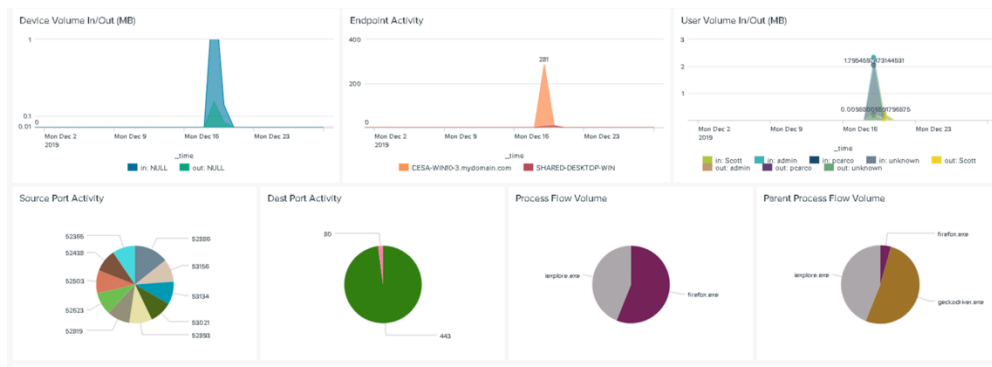
6. As I look at the graphs I see something in the parent process flow that catches my eye. It's geckodriver.exe. From here you can dig in deeper. This is a legit app but as an example maybe you don't want Firefox at all. This process is attached to Firefox.



7. Or maybe you don't want Onedrive running. So run a search on that and check out which machines are running Onedrive. Perhaps you use something company sanctioned like Code42 and that's whitelisted and want to catch all machines with Onedrive running.



8. If you scroll down further you can see what devices, applications, processes, and ports are reaching out to the site. This can help you determine if you want to control these applications further. I see geckodriver.exe is talking to Doubleclick. This doesn't seem right. Again this is just an example to showcase the different capabilities, when you get something with a more legit option.



9. Next try a search for **SSHD.exe**, you'll find this running on a Linux machine. Perhaps SSH is not allowed in your environment.

The screenshot shows the Splunk Enterprise interface for a search titled "Unapproved Applications and SaaS - Non-Whitelisted Processes". The search filters are set to "Last 30 days", "Device(s): ALL X", "Process(es): sshd X", and "Parent Process(es): ALL X". The results summary shows 1 device, 1 user, 1 process, and 1 flow. A "Flow Count Trend" chart shows 0% over a 7-day period. Below the summary is a table of flow details:

_time	Device	Platform	ose	osv	sm	User	Dst Ip	dp	Host	Src Ip	sp	Application	Parent Process
2020-05-15 15:47:12	CESA-LINUX-MACHINE	Linux	Ubuntu 18.04.4 LTS	5.3.0-76-generic	VMware, Inc.	linux-user	192.168.30.14	22	Unknown	192.168.2.13	62774	sshd	sshd

10. For those Splunkers ☺ is that what you call them? Splunk geeks you can scroll down to the flows and click on to see how the query was built and customize it



No results found. Try expanding the time range.

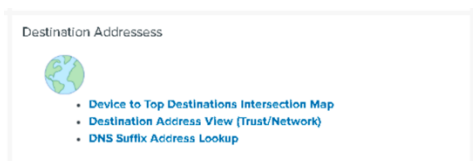
Automating this use case: These sorts of searches can be saved and made into an alert so that CESA will automatically detect these events and automatically raise an alert to the Splunk event console. Such automation is customizable for whatever data/event is important to the customer.

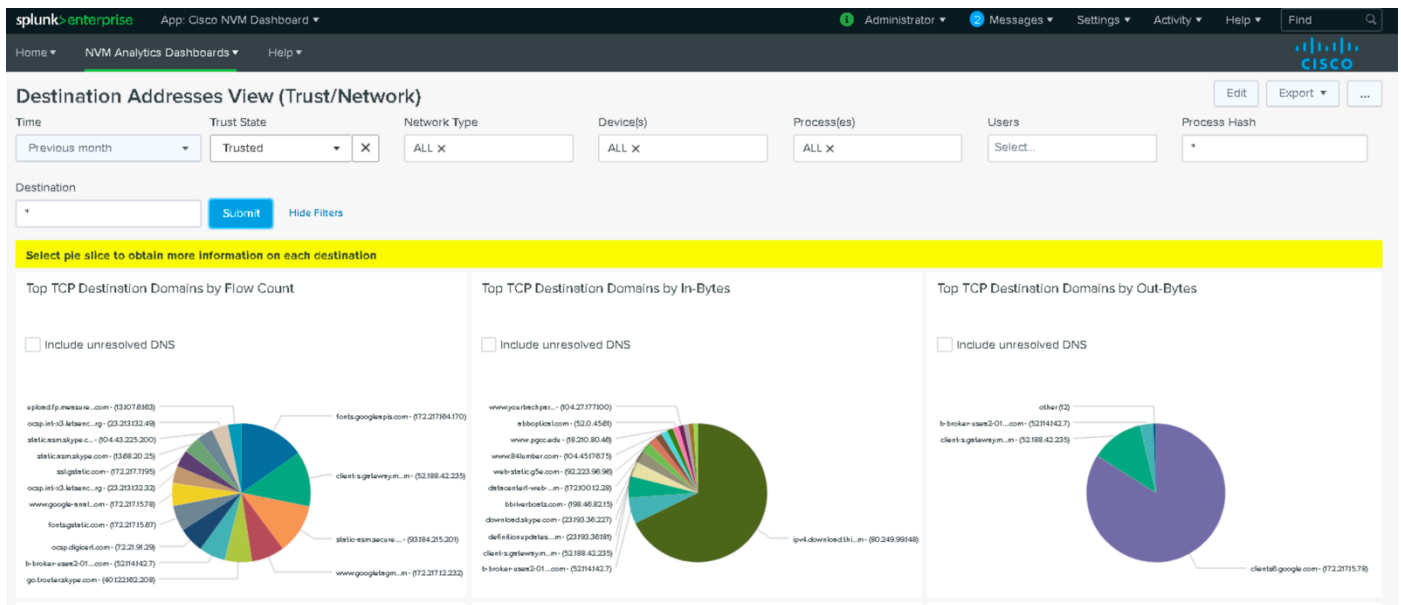
USE CASE 2b: Detecting SaaS use and abuse

Question: What SaaS is in use that I don't know about? What SaaS are there in my environment? Are they using untrusted/trusted side of the tunnel? Which side of the tunnel should they be going through if require security or already secured? What about bandwidth usage inside the tunnel vs sending it public?

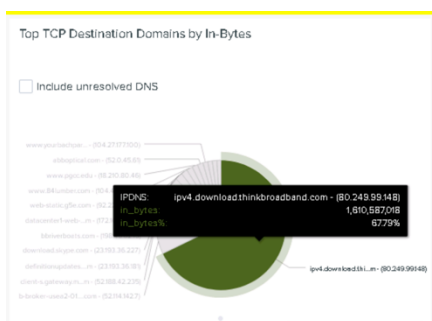
Question: Let's look into what's using up a lot of our use bandwidth on the trusted side of the interface.

1. Navigate back to the **App: Cisco NVM Dashboard**
2. Select **Destination Address View**
3. In this screen you can search through various filters to help you see what type of devices, interface (trusted/trusted), processes and users are going to different destinations. You can enter a specific domain or ip to help you filter and eventually alert on that.
4. Choose **last 30 days** which get you a good dataset.
5. Choose **trusted interface and then submit**





Our POV sample data set doesn't have a traditional SaaS service traffic in it such as Dropbox. But by way of example we can use "download.thinkbroadband.com", a service used to test broadband speeds, as an example. Hovering over Top TCP Destination Domains by In-Bytes see the data going over Trusted interface for download.thinkbroadband.com. From this example we can see that the thinkbroadband.com service actually uses a lot of bandwidth and may be something a customer would want to monitor in their environment or create policy to block it based on this CESA data.



Automating this use case: These sorts of searches can be saved and made into an alert so that CESA will automatically detect these events and automatically raise an alert to the Splunk event console. Such automation is customizable for whatever data/event is important to the customer.

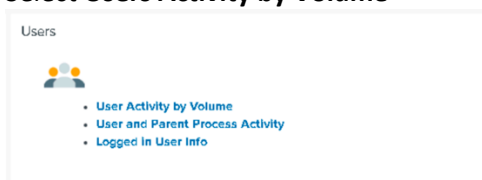
USE CASE 3: Day-Zero Malware & Threat Hunting

Question: What strange domains are being talked to and by what users and software processes?

Lsass.exe in our example below is a Windows OS system controller responsible for many OS security activities. It's a software process that you wouldn't want questionable activity around. Here we see that Lsass.exe is possibly talking to the wrong or unusual domain? For example it's ok for the process to communicate with Microsoft and Office365 domains but if it's found to be talking to another domain it maybe suspect that the exe was replaced with a bad version of it.

In the following flow we will investigate Lsass.exe by checking if it's talking to something it shouldn't be.

1. Navigate back to the **App: Cisco NVM Dashboard**
2. Select **Users Activity by Volume**

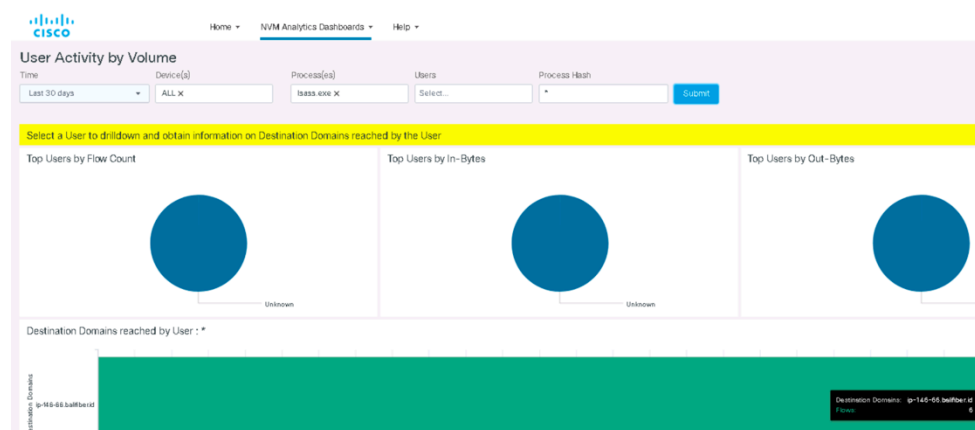


Note: By Default we will not see any events in the Dashboard because the data is over 7 days old (simulated data)

3. In the upper left change Time **last 30 days**
4. Lets filter on the process - **lsass.exe**
5. Click **Submit**

Automating this use case: These sorts of searches can be saved and made into an alert so that CESA will automatically detect these events and automatically raise an alert to the Splunk event console. Such automation is customizable for whatever data/event is important to the customer.

Notice the top domain of balifiber.id



Since we see that it's going to a bad domain. We can investigate further by looking at the application process.

In the main dashboard > Go to Application process listing

Applications

- Top Applications by Volume and Flow
- Top Source and Dest Ports
- Application Process Utilization Data
- Application Process View

Filter on **Isass.exe** and **Use last 30 days**

The screenshot shows the Splunk NVM dashboard interface. At the top, there's a filter for 'Last 30 days' and a search for 'isass.exe'. Below this, a table lists application details for 'isass.exe' with columns for Application, Platform, and Process Hash. A 'Process Hash Distribution for isass.exe' chart is visible, showing a peak in activity. To the right, a 'Table of Destinations Reached by: isass.exe' lists various domains like 'ad1.ac.factm3.com' and 'sp-145-66.barbar.id'.

Click on the **last hash** and you'll see which machine its running on

At the very bottom click on the details for the hash. This will allow you to cross launch into Virus Total, Cisco Threat Response, etc.

This screenshot shows the 'Process info view for' a specific hash: 'D42FC31AADB0E0A33F91C9513ED9110D0C181DE5B49F22615CA759AABC58'. Below the hash, there are several links for external analysis tools: ThreatGrid, Amp, Cisco Threat Response, VirusTotal, and Cisco Firepower (Host Profile).

Here I am going to click on VirusTotal. It doesn't require an account but you can try CTR if you have an account.

Virus Total will give you a report showing it's a bad process hash.

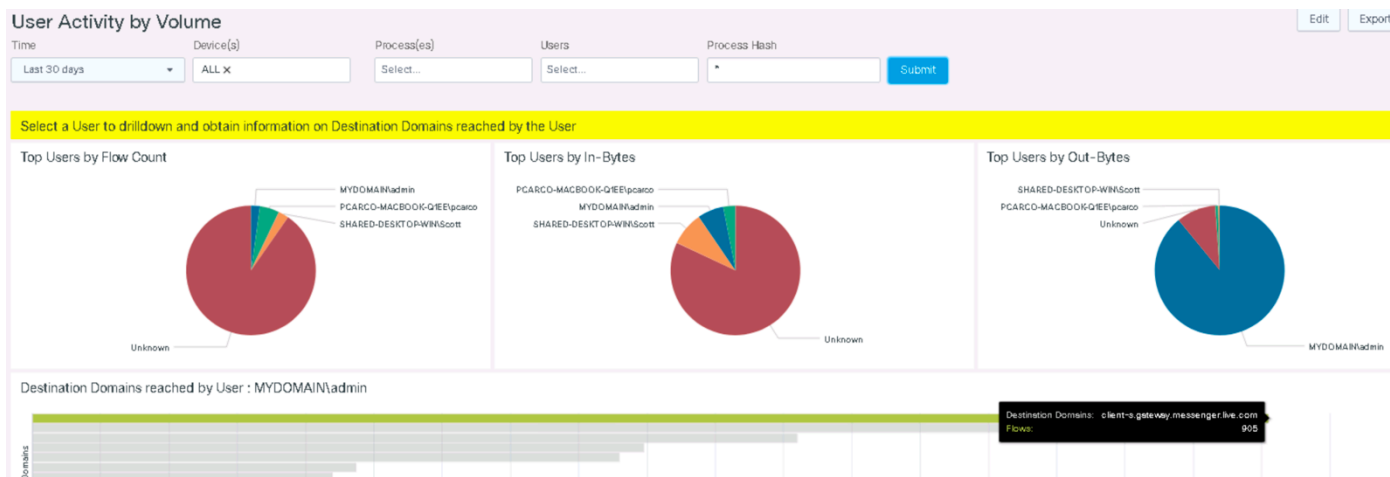
The screenshot shows the VirusTotal search results for the hash 'D42FC31AADB0E0A33F91C9513ED9110D0C181DE5B49F22615CA759AABC58'. It indicates that 49 engines detected this file. The file is identified as 'sc.exe' with a size of 279.50 KB, last updated on 2019-09-14. Below this, a table shows detection details from various engines:

DETECTION	DETAILS	COMMUNITY
Acronis	Suspicious	Ad-Aware
AegisLab	Virus Win64/Expro.nic	AbrnLab-V3
Alibaba	Virus Win64/Expro.509s4806	ALYac

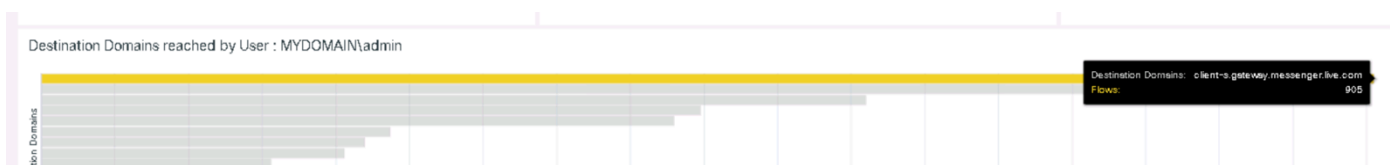
Now go back to **User Activity Volume**

For another example let's look at some of the default screen. Reset your test to check all **processes and devices**. Click into the **mydomain/admin** as it's the top use out bytes which is interesting to look into.

Search time **last 30 days**, click **Submit**



After clicking that then you can hover over the top domain. It shows Messenger running. Why is that the top domain for that user? That's a lot of communication or maybe the company doesn't want the application used for communications. Either way CESA here gives visibility to the Messenger service in use and generating a lot of traffic for this specific user.

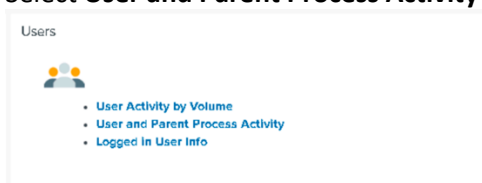


User and Parent Process

Question: What strange software processes are in use and by what users? This will allow you to get the connection between the processes and users. Let's look at localbridge.exe. Why is there only 1 user using it? And why did it show up just in the past two days?

Dig into what processes and associated users are attached to them?

1. Navigate back to the **App: Cisco NVM Dashboard**
2. Select **User and Parent Process Activity**



Note: By Default we will not see any events in the Dashboard because the data is over 7 days old (simulated data)

3. In the upper left change Time to **last 30 days**
4. Click **Apply** and then **Submit**

In this example I clicked on John (on the 2nd page of users) and it showed all the processes on his machines. I found a process running called localbridge.exe in the search and is a file known to have lots of corruptions.

Details for Process Account : SHARED-DESKTOP-WIN\John

Select a row to drilldown and obtain more information on each Application

	Process Name ↕	Parent Process Name ↕
1	apphostregistrationverifier.exe	svchost.exe
2	backgroundtaskhost.exe	svchost.exe
3	backgroundtransferhost.exe	svchost.exe
4	browser_broker.exe	svchost.exe
5	hxtsr.exe	svchost.exe
6	jp2launcher.exe	javaws.exe
7	jucheck.exe	jusched.exe
8	localbridge.exe	RuntimeBroker.exe
9	microsoftedge.exe	svchost.exe

Automating this use case: These sorts of searches can be saved and made into an alert so that CESA will automatically detect these events and automatically raise an alert to the Splunk event console. Such automation is customizable for whatever data/event is important to the customer.

Use Case 4: Data Loss Detection

Question: How can I find suspected data hoarding or exfiltration?

What is a High level of traffic to a certain domain exfiltrating data? For example Dropbox? Box? Google Drive? You can use this capability to find out. In the example below we will find a domain “bachparty” that has a large amount of data moving to it (and probably shouldn’t).

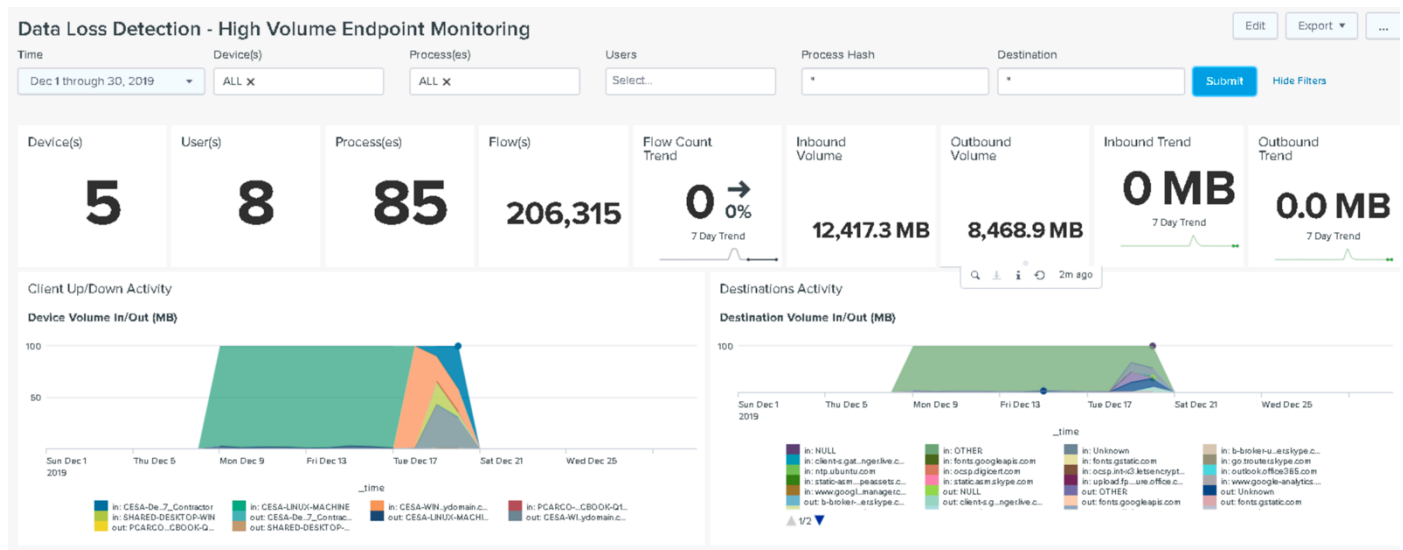
1. Return to the App: **Cisco NVM Dashboard**
2. Select **Data Loss Detection – High Volume Endpoint Monitoring**



Note: By Default we will not see any events in the Dashboard because the data is over 7 days old (simulated data)

3. In the upper left change Time Preset to **Last 30 days**
4. Click **Submit**

Automating this use case: These sorts of searches can be saved and made into an alert so that CESA will automatically detect these events and automatically raise an alert to the Splunk event console. Such automation is customizable for whatever data/event is important to the customer.



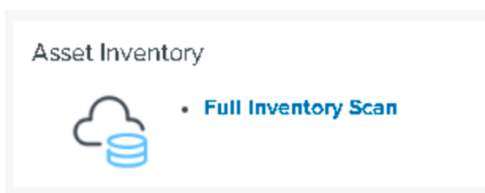
Use Case 5: Asset Inventory

Question: I want to get a summary view of OS's, device types, traffic volume, etc. on the network

This is a great breakdown and general summary view of all the devices traffic volume and OS, processes, traffic volumes as an overall summary view. It has a great ability to associate the specific NIC, even USB-attached NICs, back to a certain machine and to a specific user for powerful correlation and analysis.

Using Asset Recovery - Full Inventory Scan

1. Return to the App: **Cisco NVM Dashboard**
2. Select **Data Loss Detection**

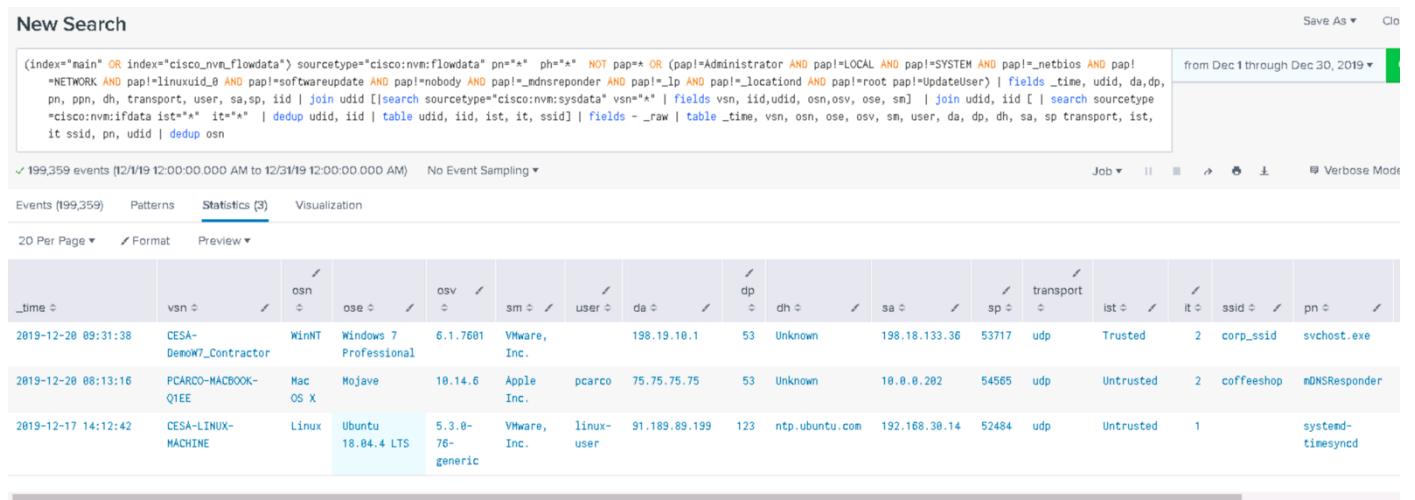


Note: By Default we will not see any events in the Dashboard because the data is over 7 days old (simulated data)

3. In the upper left change Time to Preset Last 30 days
4. Click **Apply** and then **Submit**

Automating this use case: These sorts of searches can be saved and made into an alert so that CESA will automatically detect these events and automatically raise an alert to the Splunk event console. Such automation is customizable for whatever data/event is important to the customer.

Click into the OS and then you can see that we have Windows, OSX and Linux machines as a sample. Might be new to you to know that Linux supports NVM (ISE gives you a lot of inventory with system scan posture compliance but not on Linux).



New Search Save As ▼ Clo

(index="main" OR index="cisco_nvm_flowdata") sourcetype="cisco:nvm:flowdata" pn="*" ph="*" NOT pap="*" OR (pap="Administrator AND pap="LOCAL AND pap="SYSTEM AND pap="_netbios AND pap="_NETWORK AND pap="linuxuid_0 AND pap="softwareupdate AND pap="nobody AND pap="mdnsreponder AND pap="_ip AND pap="_location AND pap="root pap="UpdateUser" | fields _time, uid, da, dp, pn, ppn, dh, transport, user, sa, sp, iid | join uid [search sourcetype="cisco:nvm:sysdata" vsn="*" | fields vsn, iid, uid, osn, osv, ose, sm] | join uid, iid [| search sourcetype="cisco:nvm:ifdata ist="*" it="*" | dedup uid, iid | table uid, iid, ist, it, ssid] | fields -_raw | table _time, vsn, osn, ose, osv, sm, user, da, dp, dh, sa, sp transport, ist, it ssid, pn, uid | dedup osn

from Dec 1 through Dec 30, 2019 ▼

✓ 199,359 events (12/1/19 12:00:00.000 AM to 12/31/19 12:00:00.000 AM) No Event Sampling ▼ Job ▼ || || | ⚙️ | 📄 | 🗨️ | 🔊 | Verbose Mode

Events (199,359) Patterns Statistics (3) Visualization

20 Per Page ▼ Format Preview ▼

<u>_time</u>	<u>vs</u>	<u>os</u>	<u>os</u>	<u>os</u>	<u>sm</u>	<u>user</u>	<u>da</u>	<u>dp</u>	<u>dh</u>	<u>sa</u>	<u>sp</u>	<u>transport</u>	<u>ist</u>	<u>it</u>	<u>ssid</u>	<u>pn</u>
2019-12-20 09:31:38	CESA-DemoN7_Contractor	WinNT	Windows 7 Professional	6.1.7601	VMware, Inc.		198.19.10.1	53	Unknown	198.18.133.36	53717	udp	Trusted	2	corp_ssid	svchost.exe
2019-12-20 08:13:16	PCARCO-HACBOOK-QIEE	Mac OS X	Mojave	10.14.6	Apple Inc.	pcarco	75.75.75.75	53	Unknown	10.0.0.202	54565	udp	Untrusted	2	coffeehop	mDNSResponder
2019-12-17 14:12:42	CESA-LINUX-MACHINE	Linux	Ubuntu 18.04.4 LTS	5.3.0-76-generic	VMware, Inc.	linux-user	91.189.89.199	123	ntp.ubuntu.com	192.168.30.14	52484	udp	Untrusted	1		systemd-timesyncd

USE CASE 6: Endpoint Security Evasion

Updated July 2020

What endpoints haven't sent endpoint security application network communications in awhile? That is an indicator that endpoint security is disabled on that endpoint.

We now have the AVG process (avgupd) included in the data set. There is a single flow record each day it is active and runs from the 1st to the 8th on a Linux machine. This way you can show it stopped on the 9th and after that.

This software process has stopped communicating with the network. CESA shows that and also shows the activity before and after the disabling of this and the ability to investigate what might have happened that caused this.

You can also look into what's not running vs what's running.

For example you could even write an alert that says if you haven't been running ampdemon in 30 days then tell me. Many different important chatty processes should be running on systems, if you don't see them then something is wrong.

In this example we are using Google application updater because we have that data available in our simulated data POV kit.

1. Return to the App: Cisco NVM Dashboard

2. Under **Security Evasion and Attribution**, select **Detection of Disabled/Inactive Endpoint Security Applications**



Note: By Default we will not see any events in the Dashboard because the data is over 7 days old (simulated data)

3. In the upper left change **Time preset 30 days**, choose **Destination avgupd**
4. Click **Submit**

Automating this use case: These sorts of searches can be saved and made into an alert so that CESA will automatically detect these events and automatically raise an alert to the Splunk event console. Such automation is customizable for whatever data/event is important to the customer.

Notice that there was some data from Google update for a while but it stopped. That means it was either purposely disabled by the user to obscure some activity they are trying to hide or that it simply stopped functioning. In either case it is a security risk on the endpoint that needs to be dealt with.

