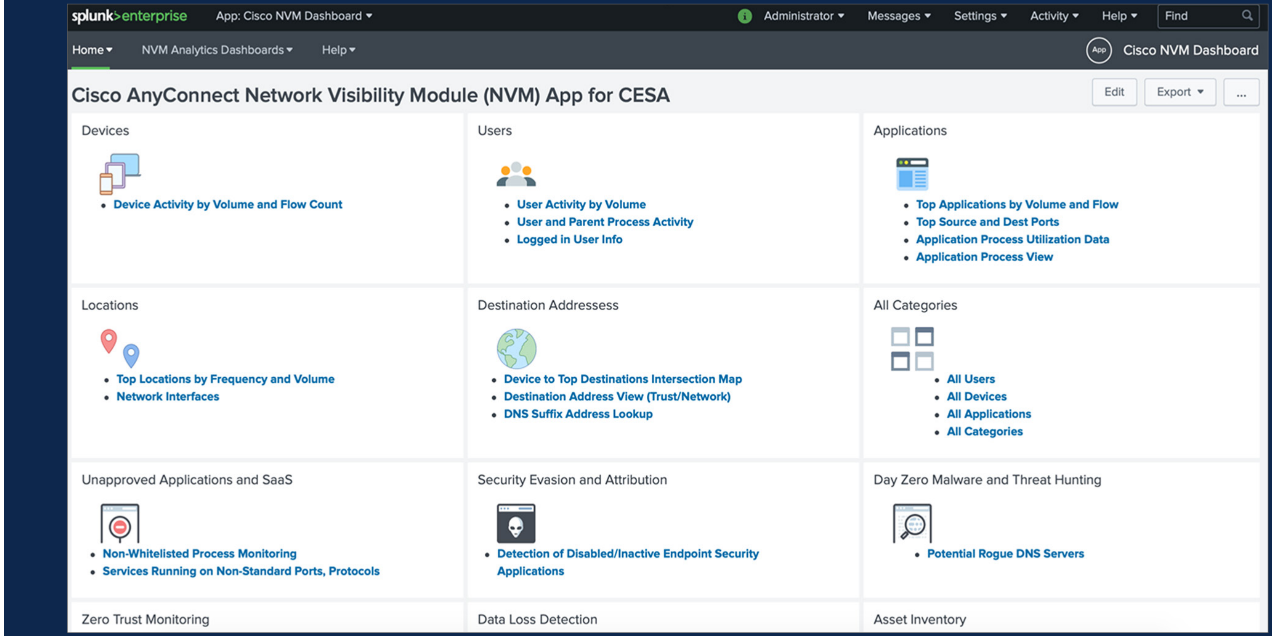
cisco
The bridge to possible

Cisco Endpoint Security Analytics Built on Splunk

Unlock deep endpoint visibility and early-warning system for threats



Cisco AnyConnect Network Visibility Module (NVM) App for CESA

Devices
- Device Activity by Volume and Flow Count

Users
- User Activity by Volume
- User and Parent Process Activity
- Logged in User Info

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

Locations
- Top Locations by Frequency and Volume
- Network Interfaces

Destination Addresssess
- Device to Top Destinations Intersection Map
- Destination Address View (Trust/Network)
- DNS Suffix Address Lookup

All Categories
- All Users
- All Devices
- All Applications
- All Categories

Unapproved Applications and SaaS
- Non-Whitelisted Process Monitoring
- Services Running on Non-Standard Ports, Protocols

Security Evasion and Attribution
- Detection of Disabled/Inactive Endpoint Security Applications

Day Zero Malware and Threat Hunting
- Potential Rogue DNS Servers

Zero Trust Monitoring

Data Loss Detection

Asset Inventory

Benefits

- **Provides endpoint device visibility:** Find endpoint threats before they're a problem–such as day-zero malware, dangerous user behavior, data exfiltration–see what applications or Software as a Service (SaaS) are in use, use forensics for incident response, and gain visibility to device types and operating systems on your network
- **Follow endpoints wherever they go:** Captures endpoint telemetry whether the device is connect to the network or off network.
- **Launches quickly and easily:** Leverage existing AnyConnect® telemetry (no new endpoint agent is required), get instant insights from the prebuilt Splunk dashboards, and conduct easy searches to ask questions and get answers.
- **Predictable costs:** Budget per endpoint instead of on variable data volume ingested into Splunk.
- **Support for diverse devices:** Windows, macOS, Linux, and Samsung Knoxenabled devices.

How CESA works

Cisco AnyConnect NVM is a module that's already part of an AnyConnect version 4.2 or later agent. NVM produces IPFIX endpoint telemetry whenever the device is in use, even when that device is off the network. This data is exported to flow collectors and forwarded to CESA Built on Splunk, where it is ingested and becomes instantly usable. With the help of a Cisco-developed Splunk NVM app, users get out-of-the-box dashboards, so they can quickly make sense of the data and start using it to answer critical security questions.

CESA may be used as a standalone NVM analytics deployment or added to an existing Splunk Enterprise environment. For standalone or greenfield deployments, CESA delivers all of the required Splunk analytics software necessary to analyze NVM telemetry. If Splunk Enterprise is already deployed, then CESA Built on Splunk provides a license for use of the NVM App and Add-on for Splunk, as well as to count your NVM endpoints separately from all other Splunk data, which provides a more cost-effective approach to analyzing NVM data in Splunk.

Cisco Endpoint Security Analytics Built on Splunk enables deep endpoint visibility

Most companies want to know what their workers and their devices are doing when they are at work, on the road or working from the coffee shop. That's why Cisco invented the AnyConnect Network Visibility Module (NVM) to provide unparalleled endpoint behavioral visibility. But endpoint devices create significant amounts of telemetry data that can be expensive to process, analyze, and understand.

So Cisco has partnered with Splunk to create Cisco® Endpoint Security Analytics Built on Splunk (CESA) to analyze AnyConnect NVM data, present it in a customized monitoring, and alert console and purchase on a per-endpoint basis for predictable, easy-to-budget costs. Now customers can understand endpoint behaviors and answer critical security questions using device telemetry data they can't get from any other security agent when they are on or off the network. CESA Built on Splunk may be deployed as a standalone NVM analytics platform or added to an existing Splunk deployment.

Powered by Cisco AnyConnect NVM and Splunk Enterprise

The AnyConnect Network Visibility Module is the only technology for mobile devices that creates IPFIX data (IP Flow Information Export) and provides rich user behavioral data, so you can see if your employees' endpoints threaten the security of your company. The behavioral data produced by NVM is complementary to antimalware agents that primarily focus on file analysis, such as Cisco Advanced Malware Protection (AMP) for Endpoints. NVM telemetry is then ingested and analyzed in CESA Built on Splunk to address endpoint security use cases such as:

Data loss detection	▪ Data hoarding activity–download and upload behavior ▪ Exfiltration–upload to external domains and network shares
Day-zero malware and threat hunting	▪ Unusual app/process behavior–running at root or on nonstandard ports ▪ Command and Control detection–burst of connections to new, unusual, or bad domain ▪ Threat detection–application process to host domain correlation
Zero-trust monitoring	▪ Off-net device monitoring–user, device, traffic, app, and data behavior ▪ SaaS use behavior–track SaaS services are being used ▪ Untrusted connections–track who is connecting to untrusted networks

Getting started–solution components

Deploying the CESA Built on Splunk solution requires:

- Generating NVM endpoint telemetry: Cisco AnyConnect Secure Mobility Client with an Apex feature license on the endpoints.
- An analytics, monitoring, and alerting dashboard: CESA Built on Splunk provides the analytics platform. Cisco NVM Technology Add-On for Splunk and Cisco AnyConnect Network Visibility Module (NVM) App for Splunk bring the NVM data into CESA and present it in a prebuilt monitoring and alerting dashboard. CESA Built on Splunk may be deployed as a standalone NVM analytics platform or added to an existing Splunk deployment.

Unapproved applications and SaaS visibility	▪ SaaS domains accessed–connections and SaaS use behavior ▪ Application and process visibility–find apps and processes running on devices
Security evasion and user attribution	▪ Endpoint security applications–detect if disabled or not installed ▪ CESA–detect if disabled or not installed ▪ Attribute user to network access–user activity down to network interface controller level
Asset inventory	▪ Device-type and OS inventory–identify and report by type ▪ Data privacy compliance–confirm removal of personal data from devices

NVM is in a class by itself for endpoint security telemetry

NVM makes AnyConnect the only security agent for mobility that uses IETF-standard IPFIX to capture, format, and transport telemetry from endpoint devices to flow collectors or network management systems for analysis and logging. As a result NVM delivers uniquely insightful endpoint telemetry such as: user, traffic direction and volume, destination of that traffic, software processes and applications present on the endpoint, SaaS services used by the endpoint, websites and domains accessed by the endpoint, and details about the device–such as device type, OS, manufacturer, and network interfaces. Security visibility and insights come from the correlation and analytics of this telemetry as performed by Splunk.

Learn more about products outlined in this brief:

- Cisco Endpoint Security Analytics Built on Splunk
- Cisco AnyConnect
- Cisco AnyConnect NVM