Cisco Endpoint Security Analytics (CESA)

Bernhard Kaiserer
Systems Engineer

Questions

1. Do you really know what's going on your Endpoints?
2. Which process is connecting to which IP/Domain?
3. Do you have the full visibility about Endpoints?
4. How quick can you find out, that there was a data breach and where?
5. Do you have an Asset Inventory?
6. Do you know which applications are installed on your Endpoints?

Cisco Endpoint Security Analytics

What is CESA?

- Combination from Cisco AnyConnect (VPN) and Splunk (Log management)

What can see CESA?

- Network data (NetFlow) and deep Endpoint information

What do I need for CESA?

- Cisco VPN AnyConnect and Splunk

How many license I need?

- Only one CESA license

Cisco AnyConnect

- Over 170M AnyConnect clients are installed, ready to collect data
- Stable and tested software
- Available for different operating system

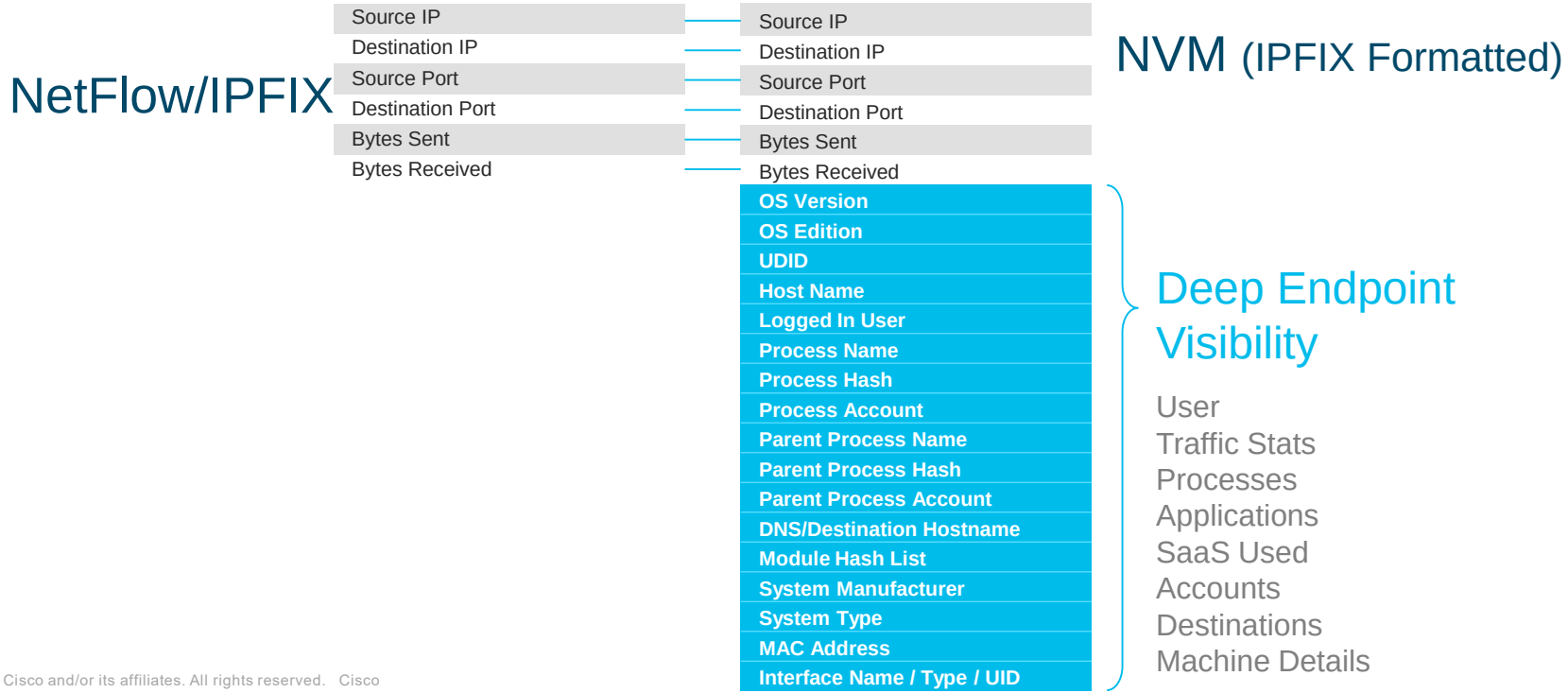
Mobile

Notebook

splunk>

Splunk is a logging, monitoring and reporting tool that makes machine data accessible and usable for users. It scans logs, metrics, and other data from applications, servers, and network devices.

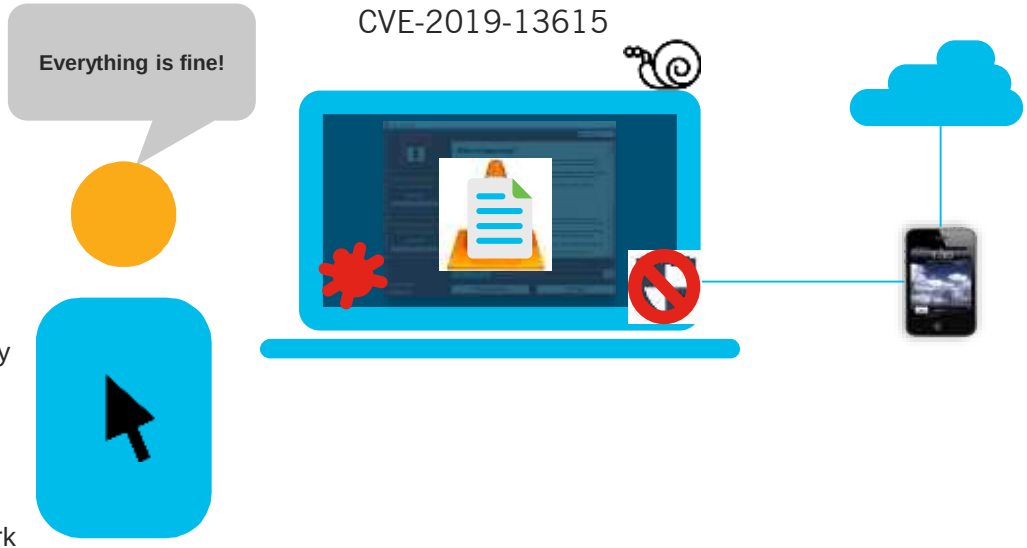
Cisco AnyConnect NVM - The Endpoint Visibility



Simple use case: Ransomware

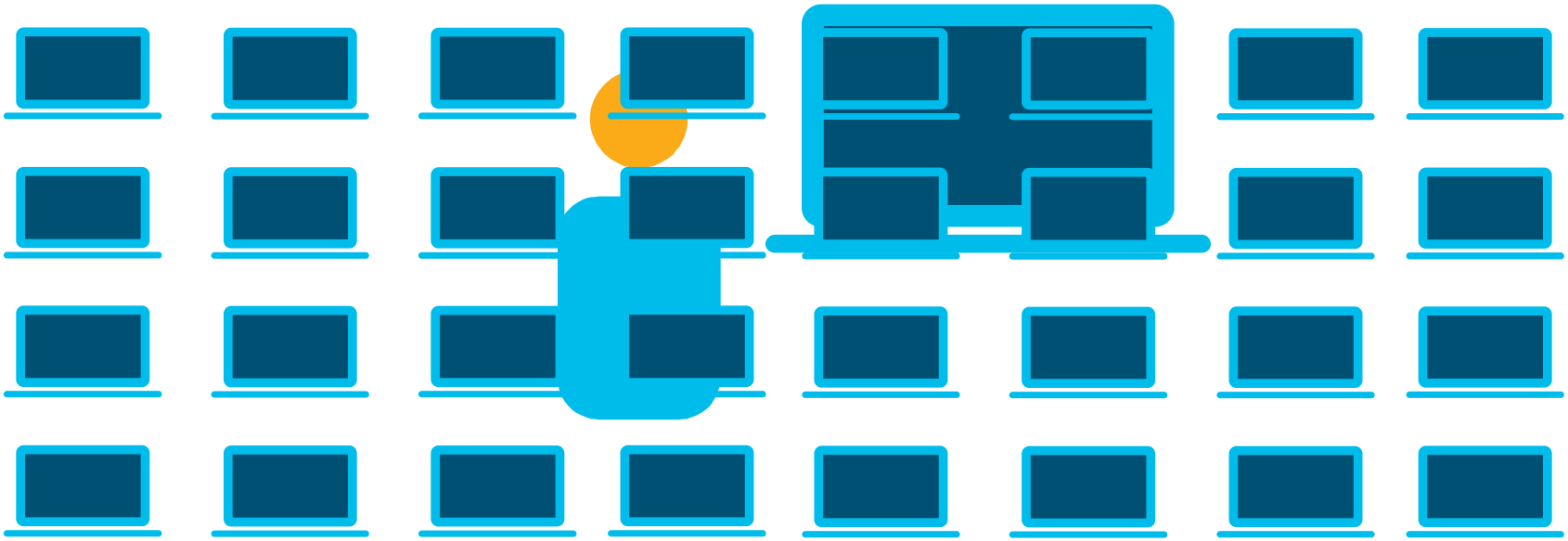
1. A user receives an unknown email
2. Ransomware encrypts files with pop up
3. User see that ransomware and need help!

Simple use case: extended Ransomware

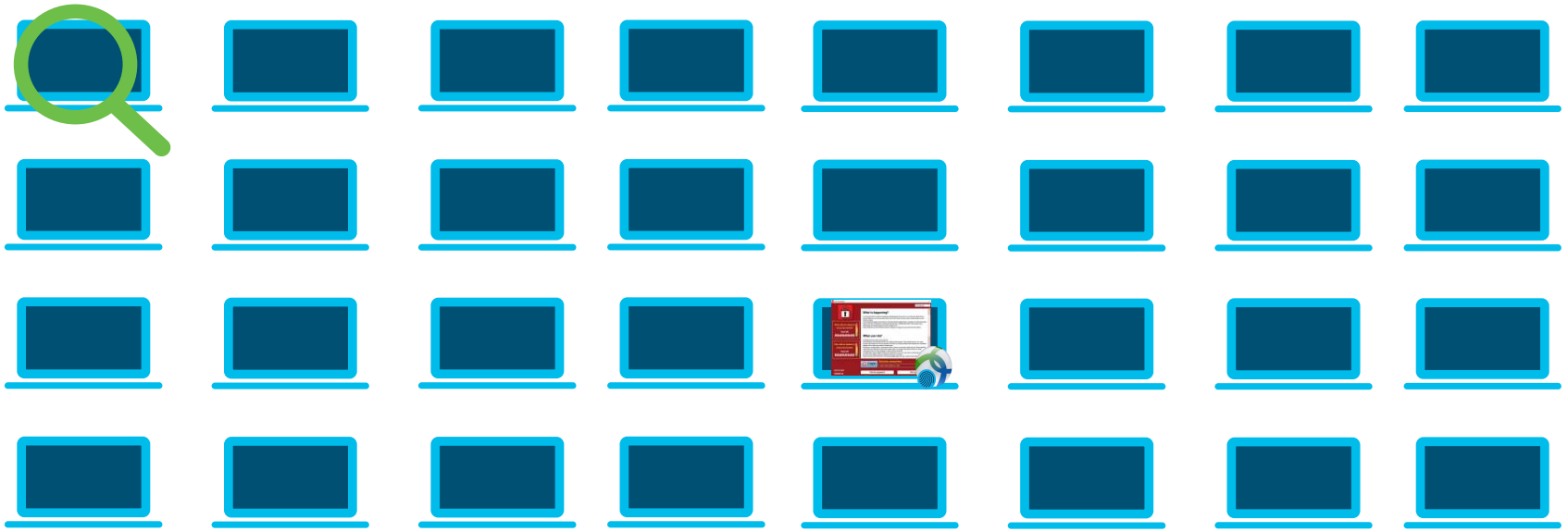


1. A user receives an unknown email
2. The computer gets slower -> endpoint security is disabled
3. The vulnerable application is opened -> the endpoint gets infected
4. The user plugs in a mobile device with network connectivity
5. Malware could upload files (C&C) -> Data Breach
6. Ransomware encrypts files without pop ups
7. User thinks that nothing changed

Simple use case: extended Ransomware



Simple use case: extended Ransomware



Simple use case: extended Ransomware

Malware Detection does not have to include **Endpoint Visibility!**

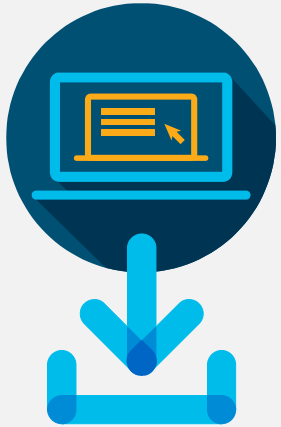
The big **customer problem** is **Endpoint Blindness!**

Example CESA Detection & Visibility Use Cases

Data Loss Detection	• Data hoarding activity – download & upload behavior • Exfiltration – upload to external domains & network shares
Unapproved Applications & SaaS	• SaaS domains accessed – connections & SaaS use behavior • Application & process visibility – find apps/processes running on devices
Security Evasion & 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 NIC level
Day-Zero Malware & Threat Hunting	• Unusual app/process behavior – running at root or on non-standard ports • C&C 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 & data behavior • SaaS use behavior – track SaaS services are being used • Untrusted connections – track who is connecting to untrusted networks
Asset Inventory	• Device-type and OS inventory – identify & report by type • Data privacy compliance – confirm removal of personal data from devices

CESA Use Case: Data Loss Detection

- **Data Loss Detection**
- Unapproved Applications & SaaS
- Security Evasion & Attribution
- Day-Zero Malware & Threat Hunting
- Zero-Trust Monitoring
- Asset Inventory



Find data hoarding & exfiltration by analyzing:

- Volume of data in motion
- Where data is going
- Who is doing it
- Endpoint involved

NVM Data Used

Source IP
Destination IP
Source Port
Destination Port
Bytes Sent
Bytes Received
OS Version
OS Edition
UDID
Host Name
Logged In User
Process Name
Process Hash
Process Account
Parent Process Name
Parent Process Hash
Parent Process Account
DNS/Destination Hostname
Module Hash List
System Manufacturer
System Type
MAC Address
Interface Name / Type / UID

CESA Use Case: Unapproved Apps/SaaS

- Data Loss Detection
- **Unapproved Applications & SaaS**
- Security Evasion & Attribution
- Day-Zero Malware & Threat Hunting
- Zero-Trust Monitoring
- Asset Inventory

SaaS

Local Applications

Find unapproved or blacklisted applications & SaaS services by analyzing:

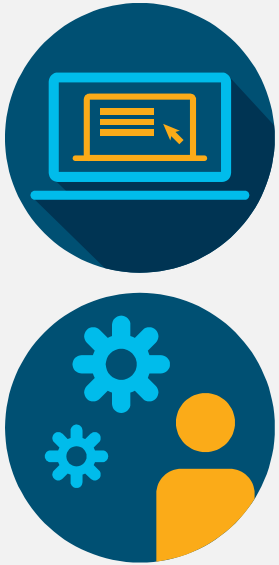
- What processes are running
- Where data is going
- Domains accessed
- Who is doing it
- Endpoint involved

NVM Data Used

Source IP
Destination IP
Source Port
Destination Port
Bytes Sent
Bytes Received
OS Version
OS Edition
UDID
Host Name
Logged In User
Process Name
Process Hash
Process Account
Parent Process Name
Parent Process Hash
Parent Process Account
DNS/Destination Hostname
Module Hash List
System Manufacturer
System Type
MAC Address
Interface Name / Type / UID

CESA Use Case: Endpoint Security Evasion

- Data Loss Detection
- Unapproved Applications & SaaS
- **Security Evasion & Attribution**
- Day-Zero Malware & Threat Hunting
- Zero-Trust Monitoring
- Asset Inventory



Find endpoints that have security functions disabled by analyzing:

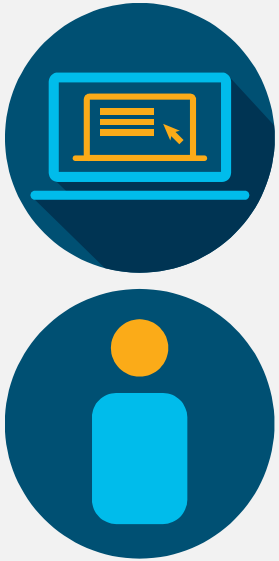
- Absence of processes running
- Absence of security telemetry sent from endpoint
- Who is the user
- Endpoint involved

NVM Data Used

Source IP
Destination IP
Source Port
Destination Port
Bytes Sent
Bytes Received
OS Version
OS Edition
UDID
Host Name
Logged In User
Process Name
Process Hash
Process Account
Parent Process Name
Parent Process Hash
Parent Process Account
DNS/Destination Hostname
Module Hash List
System Manufacturer
System Type
MAC Address
Interface Name / Type / UID

CESA Use Case: User Attribution to Activity

- Data Loss Detection
- Unapproved Applications & SaaS
- **Security Evasion & Attribution**
- Day-Zero Malware & Threat Hunting
- Zero-Trust Monitoring
- Asset Inventory



Attribute user to traffic, device & endpoint activity by analyzing:

- Who is the user
- Endpoint involved
- Network interfaces on endpoint
- Traffic direction, volume, destination & protocol
- Processes running

NVM Data Used

Source IP
Destination IP
Source Port
Destination Port
Bytes Sent
Bytes Received
OS Version
OS Edition
UDID
Host Name
Logged In User
Process Name
Process Hash
Process Account
Parent Process Name
Parent Process Hash
Parent Process Account
DNS/Destination Hostname
Module Hash List
System Manufacturer
System Type
MAC Address
Interface Name / Type / UID

CESA Use Case: Day-Zero Malware

- Data Loss Detection
- Unapproved Applications & SaaS
- Security Evasion & Attribution
- **Day-Zero Malware & Threat Hunting**
- Zero-Trust Monitoring
- Asset Inventory

Find unknown malware by analyzing:

- New or unknown domains endpoints are talking to
- Strange protocols on ports
- Unknown processes & hashes running
- Strange processes running at root
- Volume of data in motion – exfiltration & host scanning
- Endpoint system type vulnerable to type of threat

NVM Data Used

Source IP
Destination IP
Source Port
Destination Port
Bytes Sent
Bytes Received
OS Version
OS Edition
UDID
Host Name
Logged In User
Process Name
Process Hash
Process Account
Parent Process Name
Parent Process Hash
Parent Process Account
DNS/Destination Hostname
Module Hash List
System Manufacturer
System Type
MAC Address
Interface Name / Type / UID

CESA Use Case: Monitor Off-Net Activity

- Data Loss Detection
- Unapproved Applications & SaaS
- Security Evasion & Attribution
- Day-Zero Malware & Threat Hunting
- **Zero-Trust Monitoring**
- Asset Inventory

Monitor off-network behavior of endpoints by analyzing:

- User/Device-to-traffic attribution
- SaaS domains accessed
- Applications running
- Strange protocols on ports
- Volume of off-net traffic & destination
- Monitor processes, protocols & ports for unusual activity

NVM Data Used

Source IP
Destination IP
Source Port
Destination Port
Bytes Sent
Bytes Received
OS Version
OS Edition
UDID
Host Name
Logged In User
Process Name
Process Hash
Process Account
Parent Process Name
Parent Process Hash
Parent Process Account
DNS/Destination Hostname
Module Hash List
System Manufacturer
System Type
MAC Address
Interface Name / Type / UID

CESA Use Case: Devices, Apps, OSs & Privacy

- Data Loss Detection
- Unapproved Applications & SaaS
- Security Evasion & Attribution
- Day-Zero Malware & Threat Hunting
- Zero-Trust Monitoring
- **Asset Inventory**

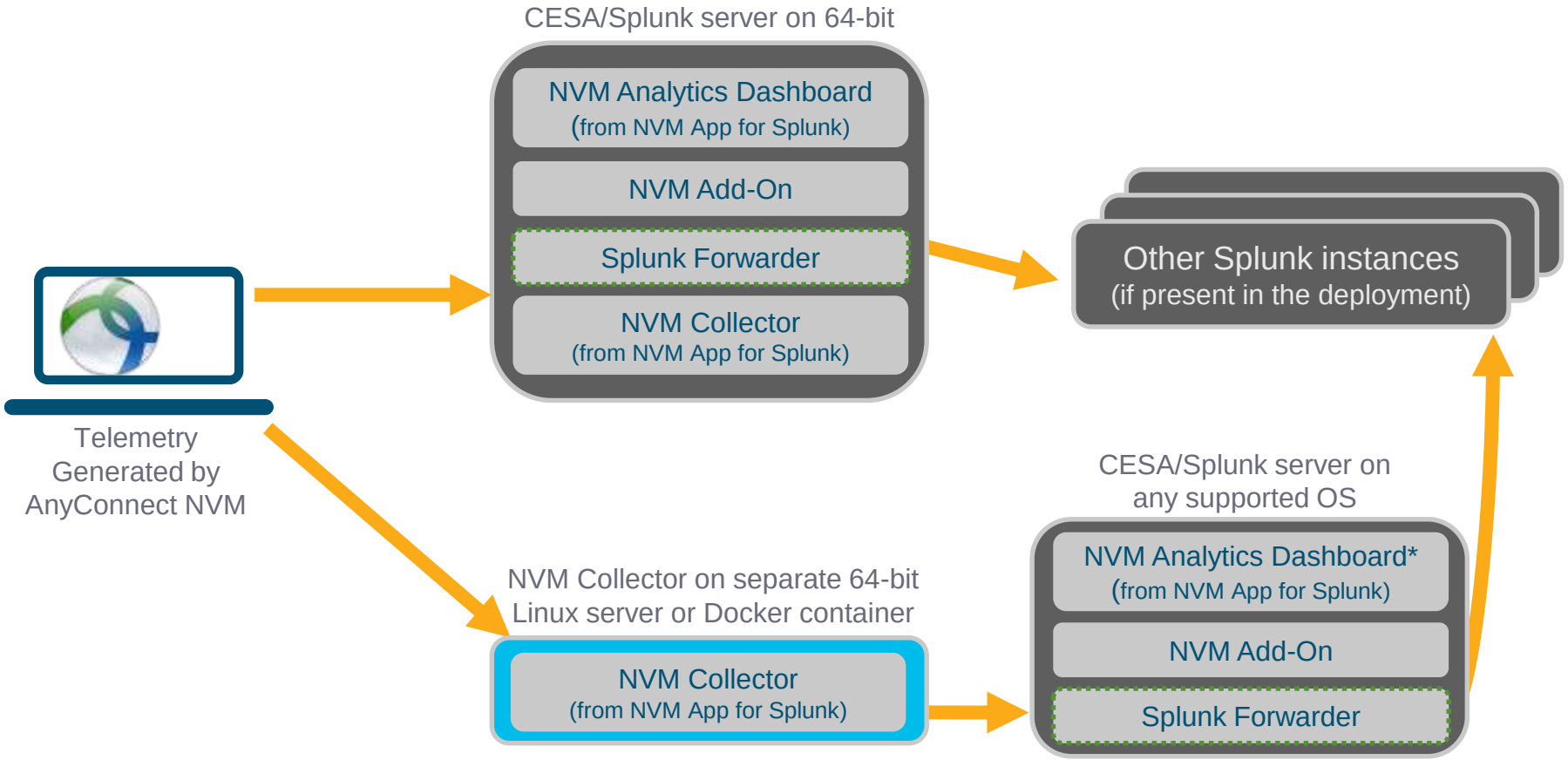
Take inventory of all OS/versions, device-types & privacy compliance in the org by analyzing:

- OS & version installed
- Applications installed
- Device-type
- Device manufacturer
- Attributing network interfaces that belong to the endpoint
- User account data wiped from device

NVM Data Used

Source IP
Destination IP
Source Port
Destination Port
Bytes Sent
Bytes Received
OS Version
OS Edition
UDID
Host Name
Logged In User
Process Name
Process Hash
Process Account
Parent Process Name
Parent Process Hash
Parent Process Account
DNS/Destination Hostname
Module Hash List
System Manufacturer
System Type
MAC Address
Interface Name / Type / UID

Deployment Architecture



Taking Action on Threats & Compliance Issues Found by CESA

Threats & Compliance Issues Detected by CESA

- Data Loss Detection
- Unapproved Applications & SaaS
- Security Evasion & Attribution
- Day-Zero Malware & Threat Hunting
- Zero-Trust Monitoring
- Asset Inventory

Remediation & Response Actions

Cisco ISE
Rapid Threat Containment from CESA/Splunk Console

User/Device Investigation and Quarantine

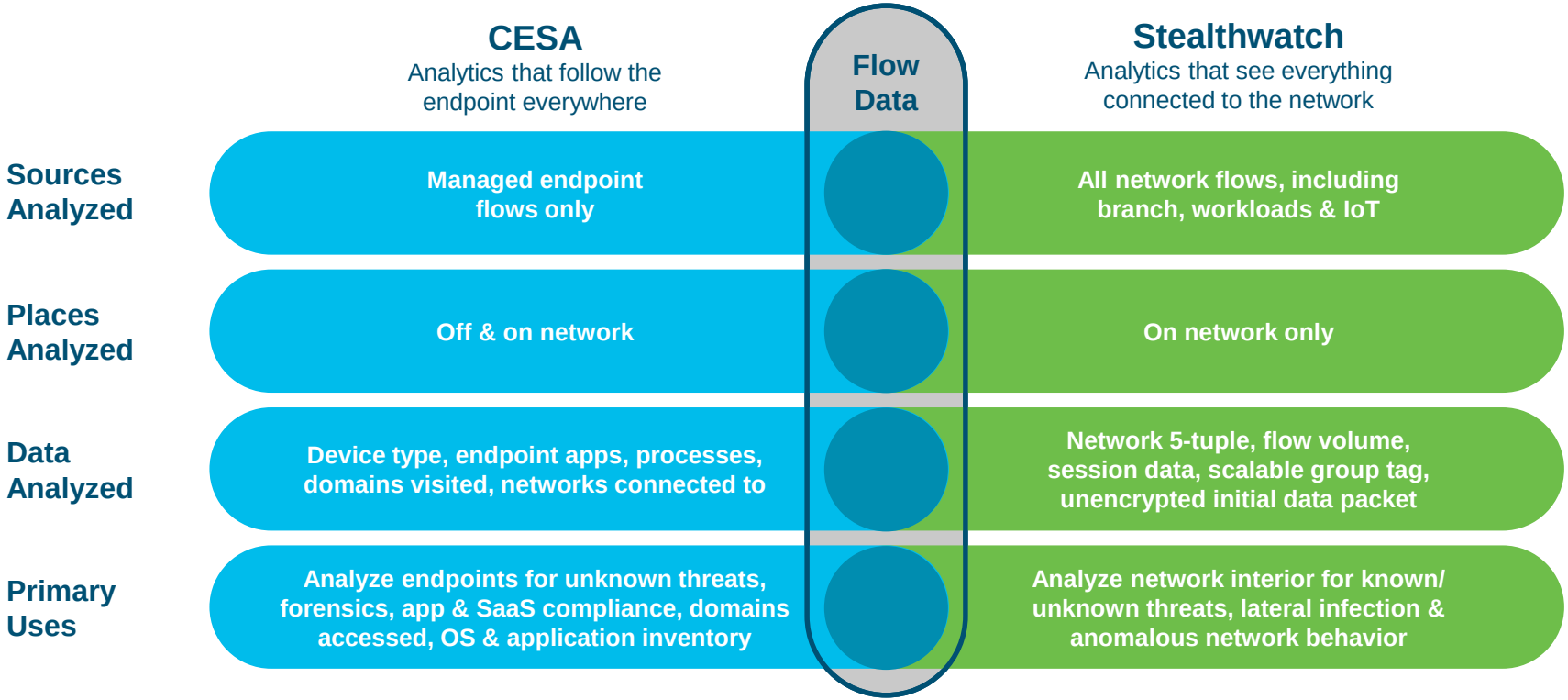
Cisco Umbrella
Enforcement from CESA/Splunk Console

Blocks Malicious Destinations

Cisco AMP
Endpoint Enforcement from AMP Console

Endpoint File Revocation, Process Termination

A More Complete Picture with Network & Endpoint Flows



Unlock deep endpoint visibility and early-warning system for threats

cisco.com/go/cesa

Thank you for your attention!

cisco.com/go/cesa