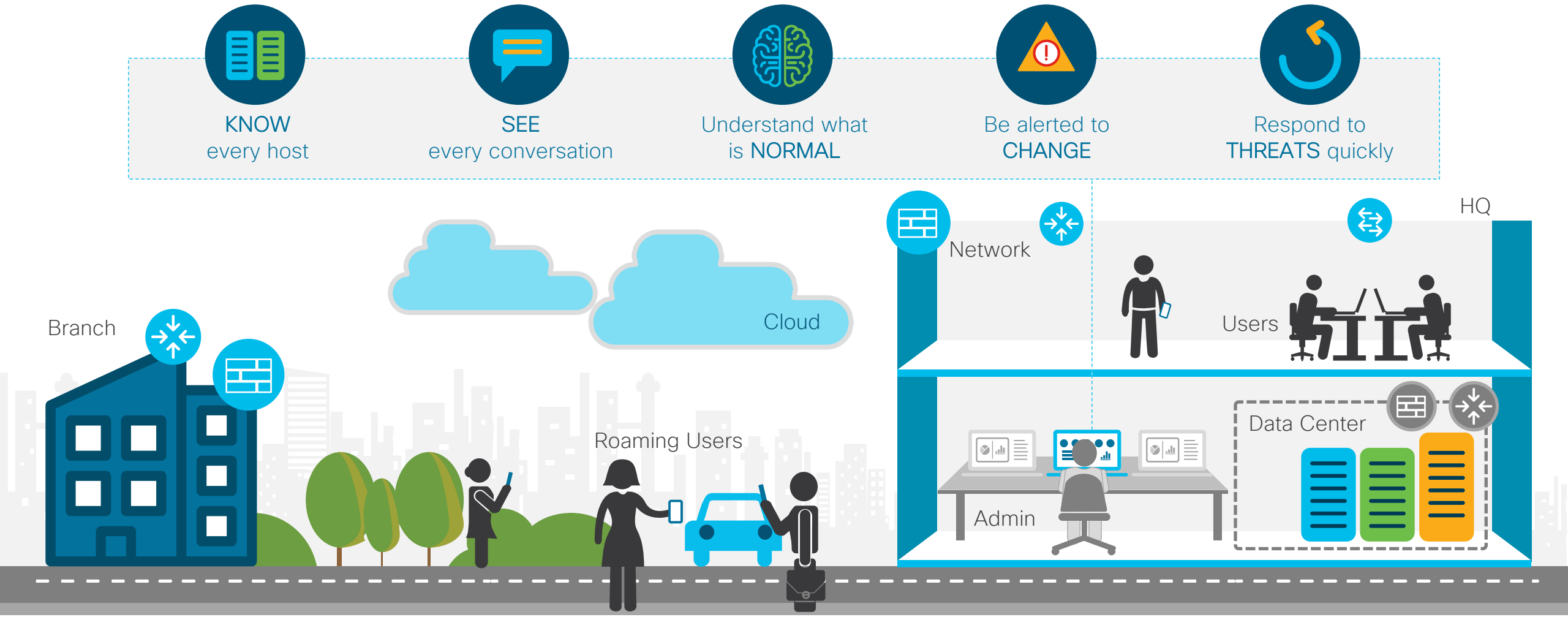
AJ Shah

Scalable Visibility and Security analytics

Effective security depends on total visibility



Stealthwatch provides the security visibility you need

Stealthwatch Enterprise

Enterprise network monitoring

- On-premises network monitoring
- Suitable for enterprises & large businesses
- On-premises virtual or hardware appliance

Stealthwatch Cloud

Public cloud monitoring

- Public cloud monitoring
- Suitable for enterprises & commercial businesses using public cloud services
- Software as a Service (SaaS)

Private network monitoring

- On-premises network monitoring
- Suitable for SMBs & commercial businesses
- Software as a Service (SaaS)

Use case/Functionality	Stealthwatch Enterprise		Stealthwatch Cloud	
	Available today	Roadmap	Available today	Roadmap
Public cloud monitoring		✔	✔	
On-prem network monitoring	✔		✔	
Dynamic entity modeling	✔[1]	✔*	✔	
Host/Entity Groups	✔			✔*
Threat detections	✔		✔	
Policy violations	✔		✔[2]	✔*
Custom Security Events	✔		✔[2]	✔
ISE user and device attribution	✔		✔[3]	✔
ISE Remediation/Mitigation	✔			✔
ISE Network Segmentation	✔			✔
Extendable hot storage	✔		✔	
Extendable long-term cold storage		✔		✔
Response Management – Emails Syslog, APIs	✔		✔	
Cisco Threat Response	✔			✔*
SecureX	✔**		✔**	
Alarm/Alert Customization	✔		✔[2]	✔
NetOps Monitoring	✔		✔[2]	✔
Forensics	✔		✔	
Threat Intelligence	✔		✔	
Encrypted Traffic Analytics: Malware Detection	✔		✔	
Encrypted Traffic Analytics: Cryptographic Audit	✔		✔	
NAT/Load Balancer/Proxy support	✔			
Endpoint telemetry and alerting	✔			✔
Firewall log storage and alerting		✔*	✔	

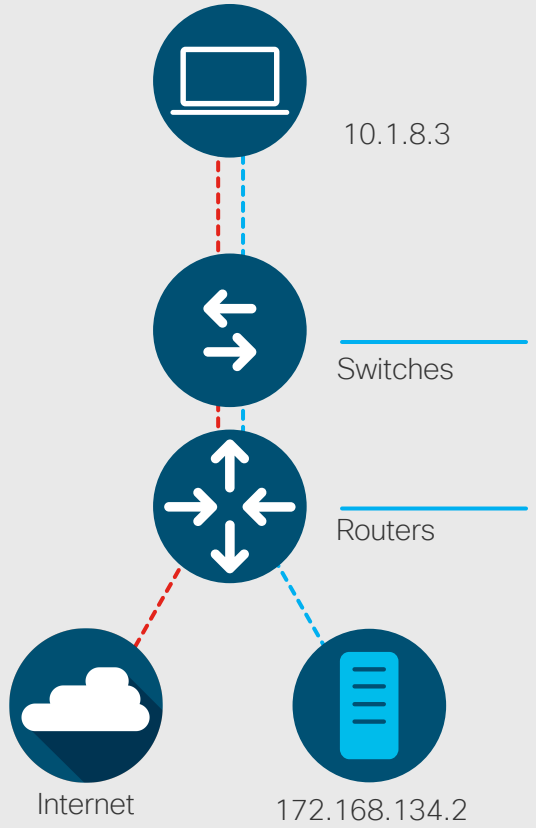
✔[1] Based on IP only
[2] Limited

✔* In current development
** At Launch

The network is a valuable data source

What it provides:

- A trace of every conversation in your network
- Collection of records all across the network (routers, switches, firewalls)
- Network usage metrics
- Ability to view north-south as well as east-west communication
- Lightweight visibility compared to Switched Port Analyzer (SPAN)-based traffic analysis
- Indications of compromise (IOC)
- Security group information

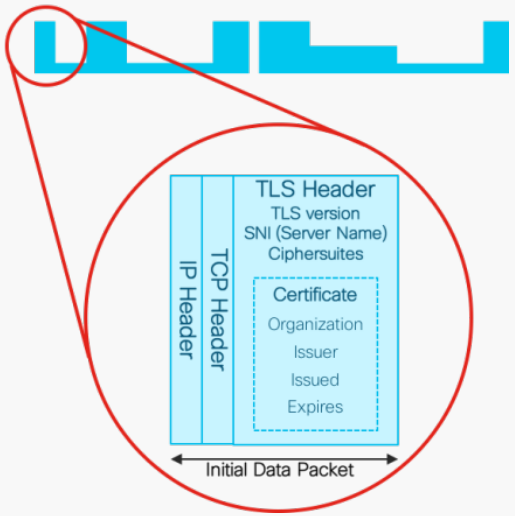


Flow Information	Packets
SOURCE ADDRESS	10.1.8.3
DESTINATION ADDRESS	172.168.134.2
SOURCE PORT	47321
DESTINATION PORT	443
INTERFACE	Gi0/0/0
IP TOS	0x00
IP PROTOCOL	6
NEXT HOP	172.168.25.1
TCP FLAGS	0x1A
SOURCE SGT	100
:	:
APPLICATION NAME	NBAR SECURE-HTTP

How can we inspect Encrypted Traffic?

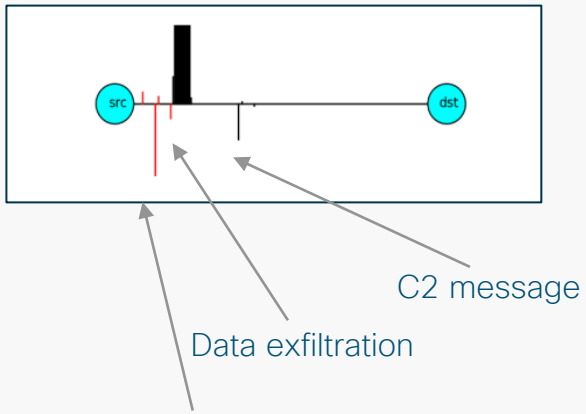
Initial data packet

Make the most of the unencrypted fields



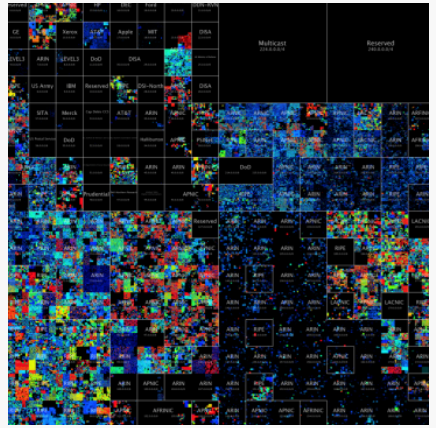
Sequence of packet lengths and times

Identify the content type through the size and timing of packets



Global risk map (Cognitive)

Who's who of the Internet's dark side

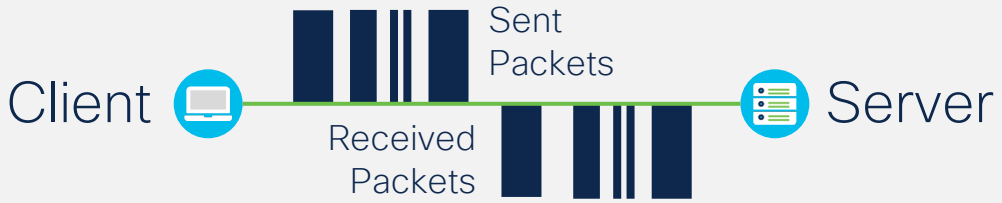


Broad behavioral information about the servers on the internet.

Identifying malicious encrypted traffic

Higher efficacy with new data

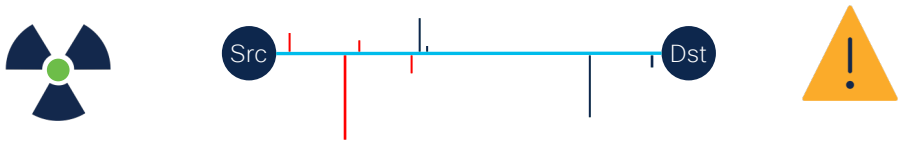
Model



Packet lengths, arrival times and durations tend to be inherently different for malware than benign traffic

Google search page download

Initiate command and control



Exfiltration and keylogging

Required core components

Secure Network Analytics management console

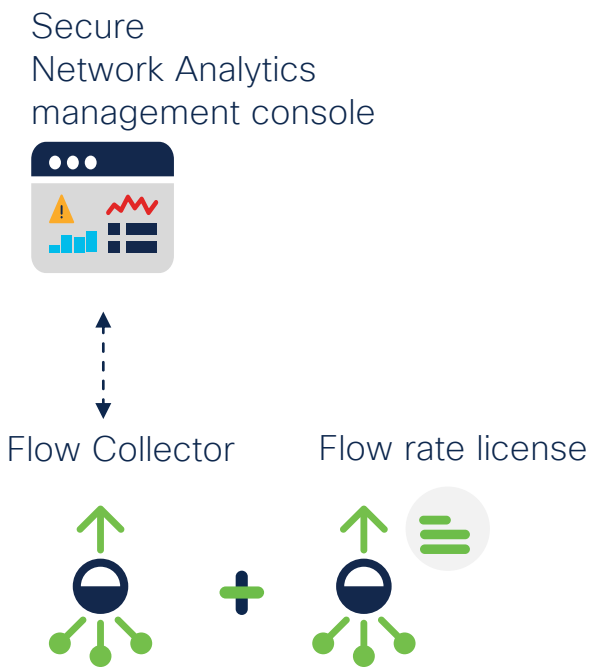
- A physical or virtual appliance that aggregates, organizes, and presents analysis from flow collectors
- Central management for all Secure Network Analytics devices
- User interface to Secure Network Analytics
- Maximum 2 per deployment

Flow collector (FC)

- A physical or virtual appliance that aggregates, normalizes and analyze telemetry and application data collected from exporters such as routers, switches, and firewalls
- High performance NetFlow/SFlow/IPFIX collector
- Maximum 25 per deployment

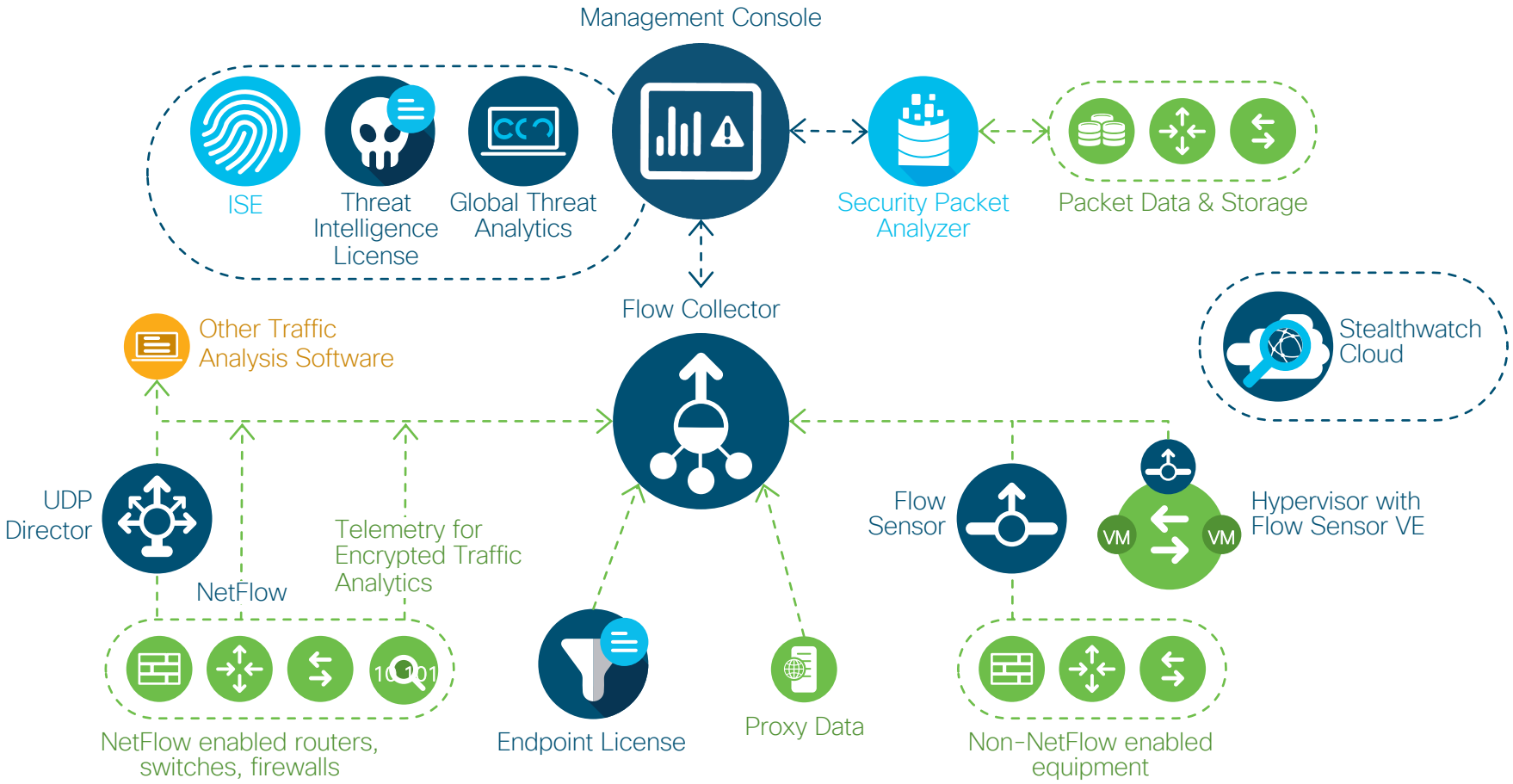
Flow rate license

- Collection, management, and analysis of telemetry by Secure Network Analytics
- The flow rate license is simply determined by the number/type of switches, routers, firewalls and probes present on the network
- FPS estimation Tool
  https://apps.cisco.com/cfgon/public/app/lancope/fpsestimator.jsp#/add-items



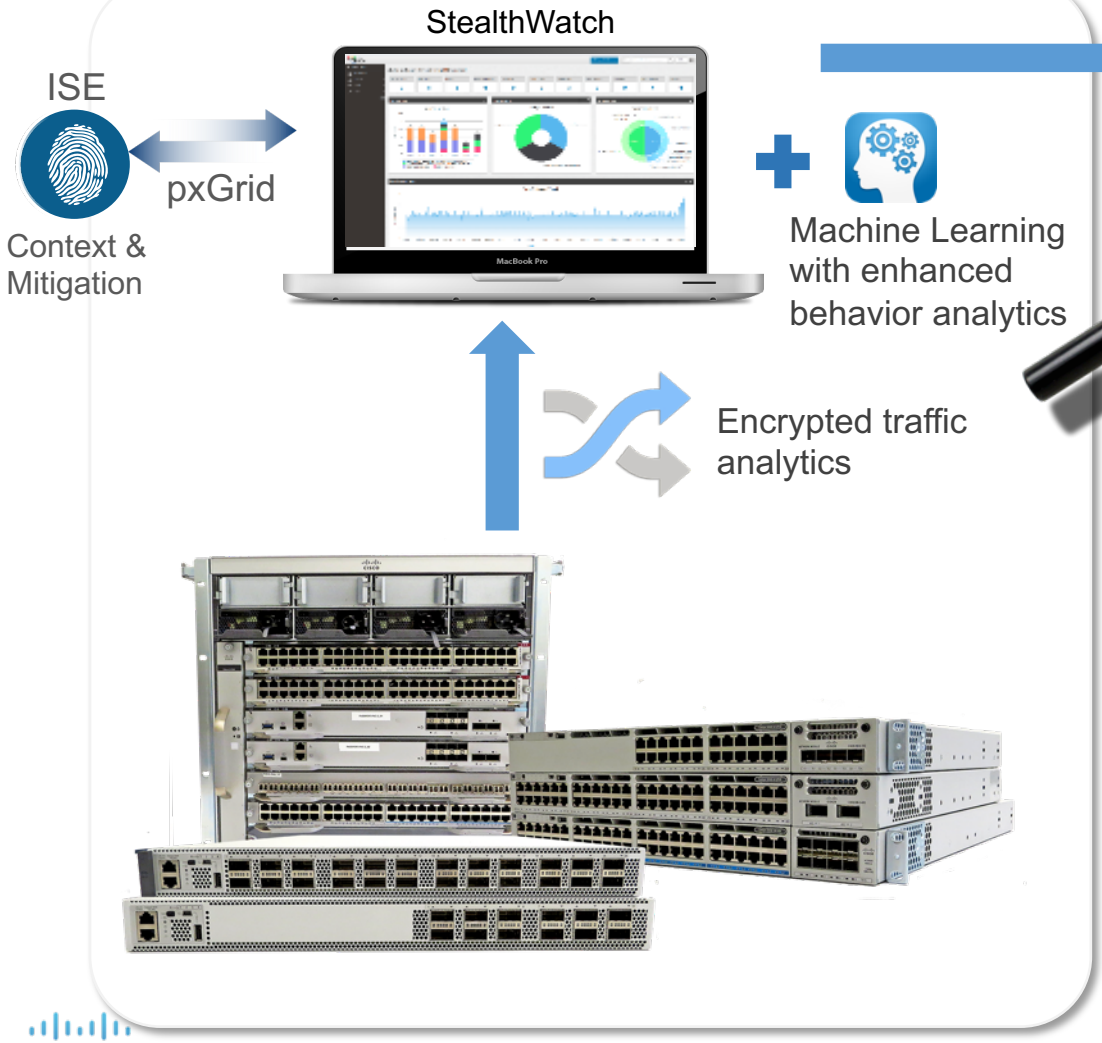
Stealthwatch Enterprise architecture

Comprehensive visibility and security analytics



Catalyst 9K Enables Enhanced Network as a Sensor and Enforcer

Analytics to Identify Malware in Encrypted Traffic *Without Decryption* & Respond



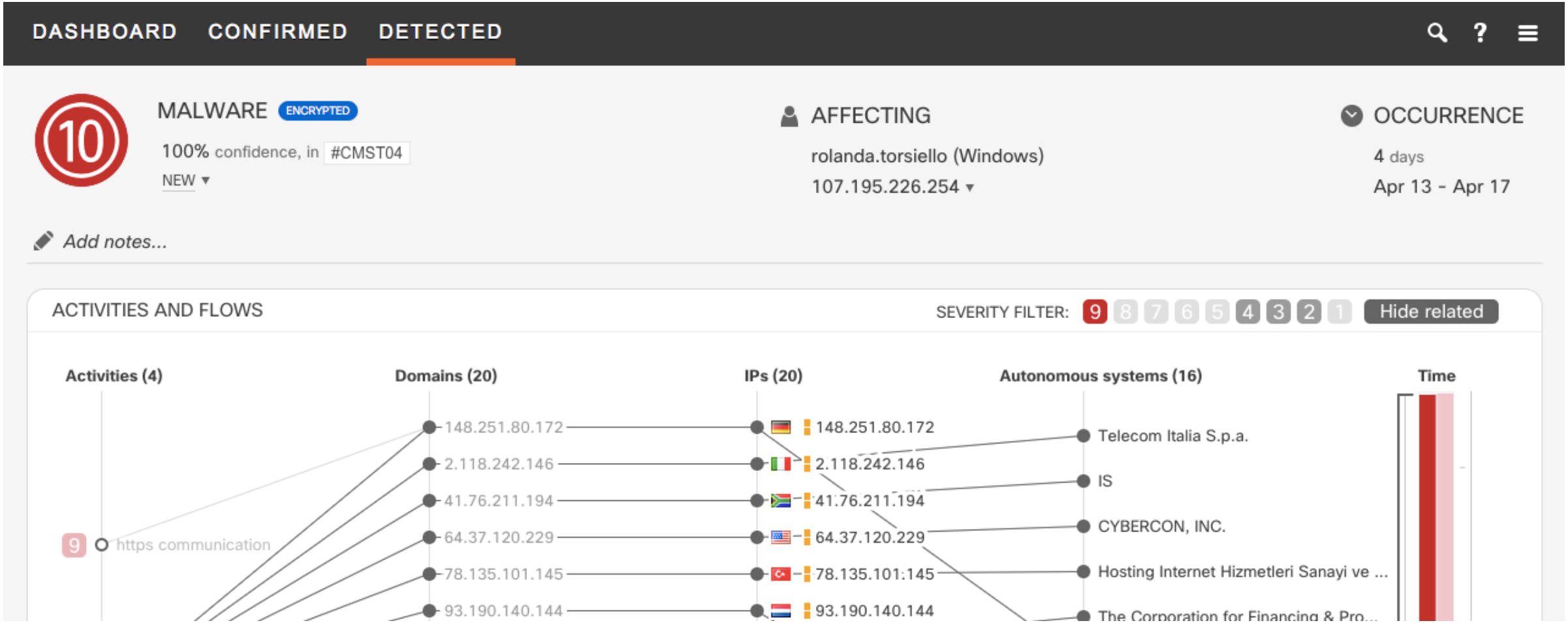
Analytics indicating Malware in Encrypted Traffic @ 99+% Efficacy

- Network Telemetry based (No Decryption)
- Line Rate Performance
- Investment Optimization
- Simplified Management
- Globally correlated threat intel

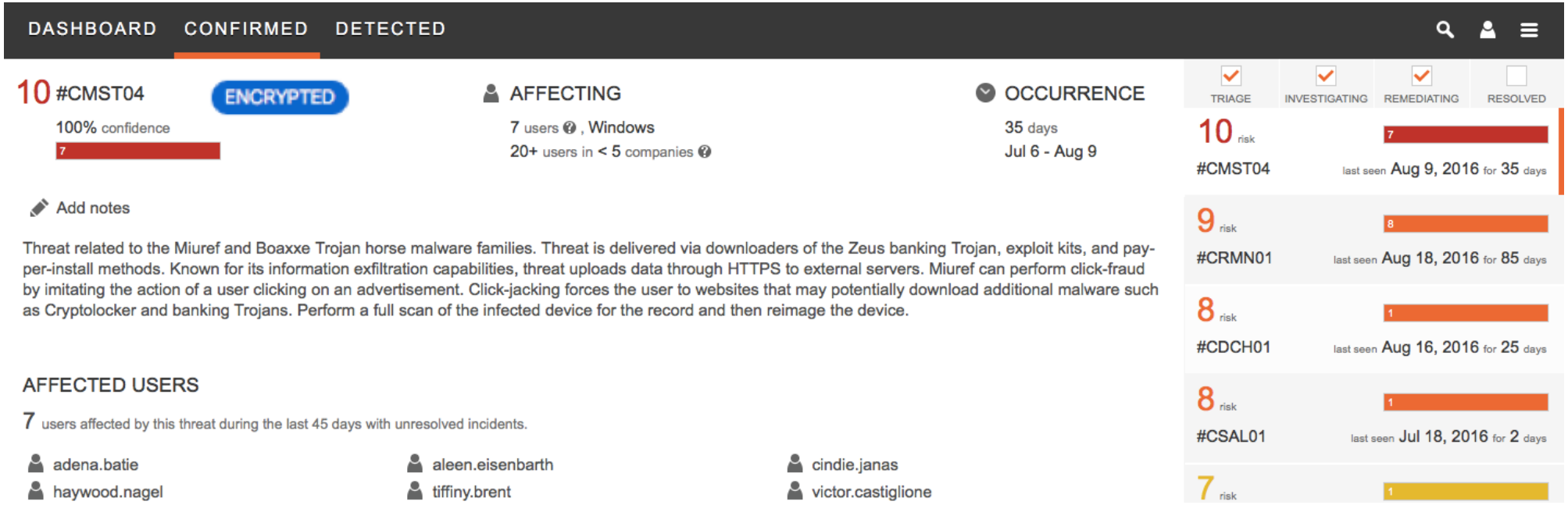
Mitigation using ISE & Network

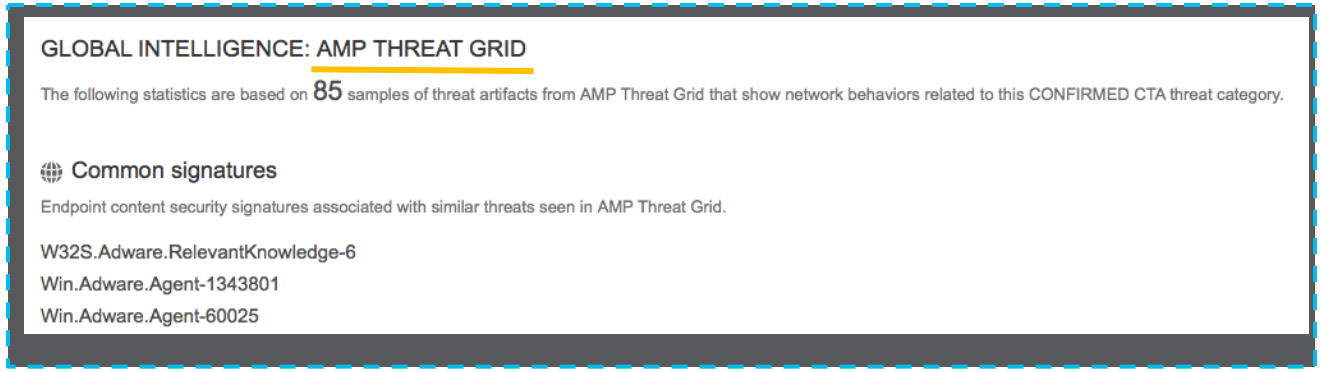
ERSPAN to send traffic for deeper analysis

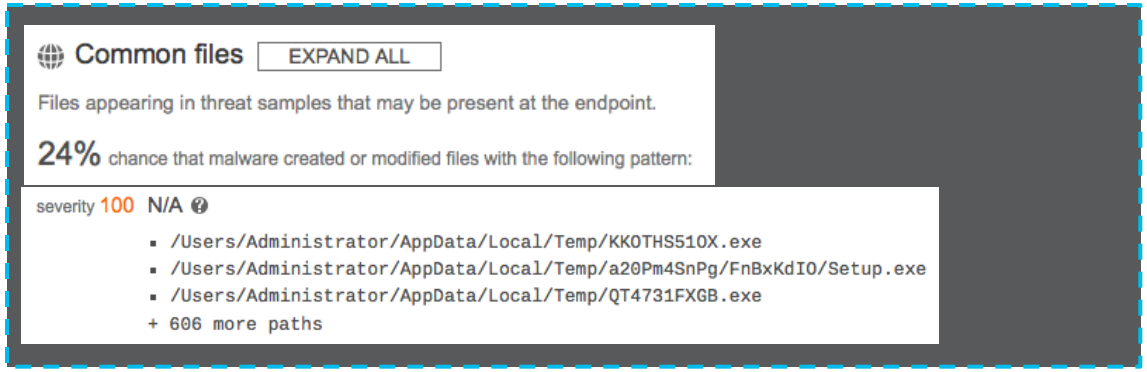
Encrypted Traffic Analytics: Example Incident



Cognitive Analytics: Confirmed Threats







Stealthwatch Value Use Case Menu

This limited collection of use cases highlights the capabilities of Stealthwatch

Threat Detection

- ☐ Detecting Beaconing
- ☐ Detecting Bogon Traffic
- ☐ Detecting Command and Control Traffic Using the Threat Intelligence License
- ☐ Detecting Fake Applications
- ☐ Detecting Fileless Malware – PowerShell Attacks
- ☐ Detecting Internal Brute Force Attacks
- ☐ Detecting Lateral Movement
- ☐ Detecting Man in the Middle Attacks
- ☐ Detecting Password Spray Attacks
- ☐ Detecting Rogue DHCP Servers
- ☐ Detecting Tor Traffic
- ☐ Detecting Rogue DNS Traffic
- ☐ Detecting Fragmentation Attacks
- ☐ Detecting Targeted Attacks
- ☐ Detecting ATM Attacks
- ☐ Detecting WannaCry Malware
- ☐ Reducing Mean Time To Know
- ☐ Detecting Browser-Based Attacks
- ☐ Detecting Cryptomining Attacks
- ☐ Using Cognitive Intelligence
- ☐ Using Cognitive Intelligence and AMP for Network Security
- ☐ Detecting Malware in Encrypted Traffic

Stealthwatch Cloud

- ☐ Investigating IP and Port Scans Using Stealthwatch Cloud
- ☐ Investigating Potential Data Exfiltration Using Stealthwatch Cloud
- ☐ Investigating Potential Threats Using Stealthwatch Cloud
- ☐ Monitoring Cloud Resources Using Stealthwatch Cloud
- ☐ Detecting Endpoint Deviations Using Stealthwatch Cloud

Compliance

- ☐ Identifying Medical Asset Types on the Network
- ☐ Managing Stealthwatch Users
- ☐ Monitoring Trusted Third Parties
- ☐ Using Bi-Directional Policies
- ☐ Using the ETA Cryptographic Audit Application
- ☐ Using the Visibility Assessment Application
- ☐ Verifying Change Control Management
- ☐ Detecting Obsolete Encryption Protocols
- ☐ Detecting Insecure Protocols
- ☐ Detecting Torrent or File Sharing Traffic
- ☐ Monitoring Vendor Activity
- ☐ Monitoring High Priority Host Groups
- ☐ Detecting Fake Applications
- ☐ Detecting Rogue and New Devices
- ☐ Defining Business Applications
- ☐ Detecting Application Access Policy Violation
- ☐ Identifying Applications on the Network
- ☐ Monitoring Remote Access Users
- ☐ Using Custom Security Events to Monitor Firewalls
- ☐ Using Encryption Auditing

Incident Response

- ☐ Determining if a User Violated Access Policies
- ☐ Detecting Users Not Traversing the Web Proxy
- ☐ Detecting Unauthorized Hosts in a Bypass VLAN
- ☐ Determining if Internet Hosts are Connecting to Internal Servers
- ☐ Monitoring Corporate Email
- ☐ Using the SMC Web UI for Threat Investigation
- ☐ Detecting Top Alarming Hosts on the Network

Network Visibility

- ☐ Identifying a Virtual Machine Generating Excessive Traffic
- ☐ Investigating NTP Reflection DDoS
- ☐ Investigating Unidirectional Traffic
- ☐ Using the Host Classifier Application
- ☐ Using the Interface Status Report in the SMC Web UI for Network Operations
- ☐ Using the SMC Web UI for Network Usage Accounting
- ☐ Using Stealthwatch for Network Segmentation and Policy Development

Forensic Investigation

- ☐ Reporting Internet URL Access
- ☐ Using the Interface Status Report for Security Operations
- ☐ Using the Security Event Workflow
- ☐ Using Top Reports
- ☐ Obtaining Historical Conversations for Unauthorized Data Transfer

Alarm Categories

- ☐ Alarm Category: Command and Control
- ☐ Alarm Category: Anomaly
- ☐ Alarm Category: Recon
- ☐ Alarm Category: High Concern and High Target Index
- ☐ Alarm Category: Data Exfiltration
- ☐ Alarm Category: Policy Violation
- ☐ Alarm Category: Data Hoarding
- ☐ Alarm Category: DDoS
- ☐ Alarm Category: Exploitation

Published October 2019

Stealthwatch: A use case approach to solving crucial network security gaps

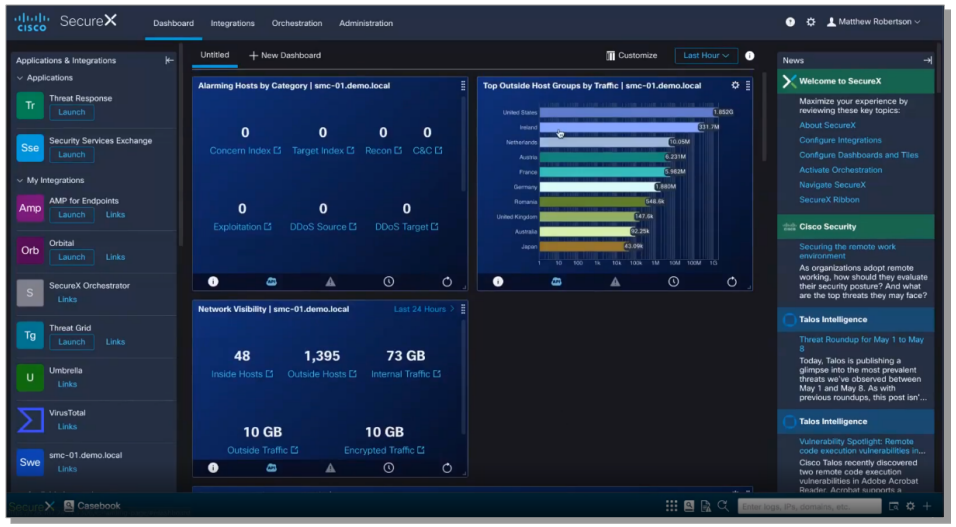
Find the use case docs at:

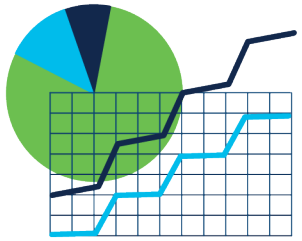
cs.co/StealthwatchValueUseCaseMenu

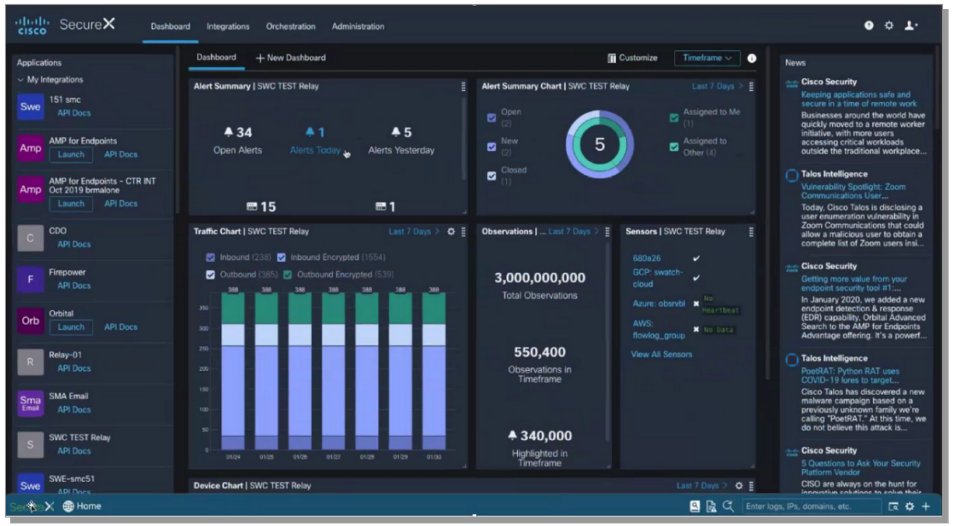
Secure Network Analytics dashboards in SecureX

Dashboard

- Alarming hosts by category
- Top outside host groups by traffic
- Network visibility
- Top inside host groups by traffic
- Visibility assessment
- Top alarms by count
- Top alarming hosts



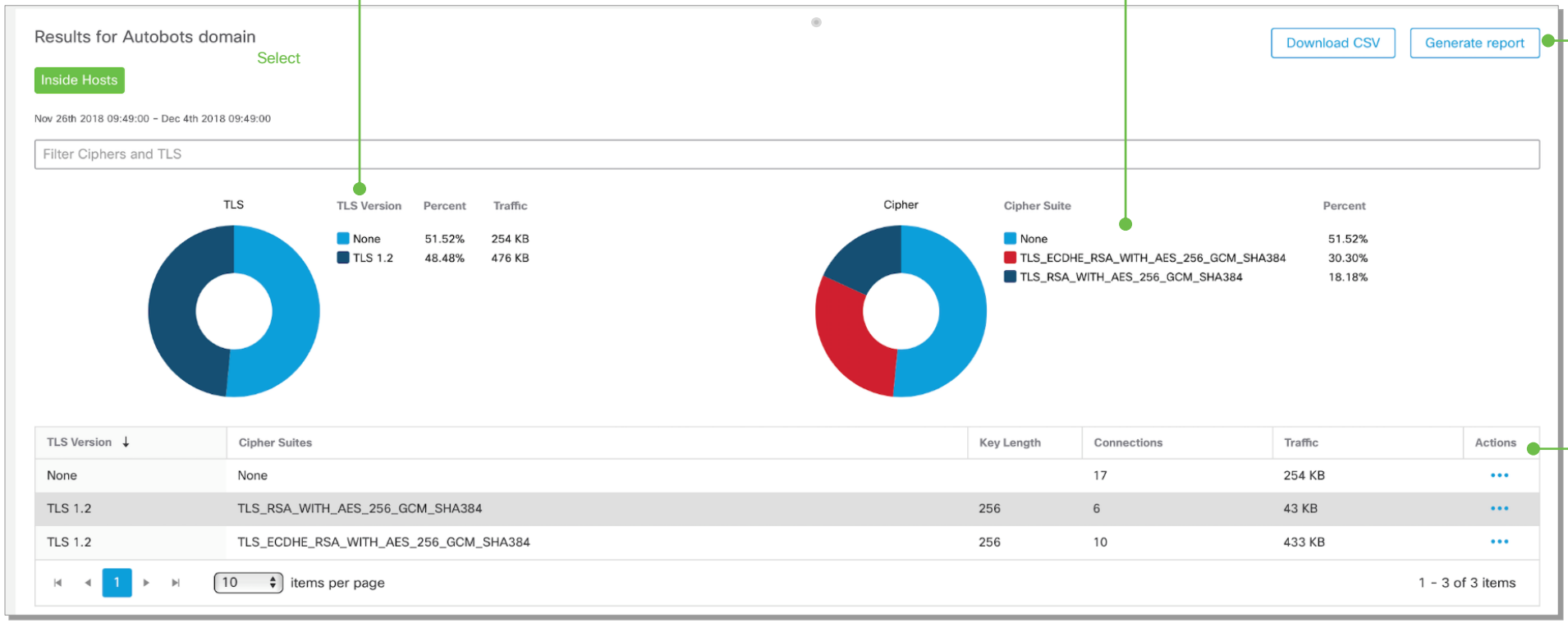




Crypto compliance reporting

By SSL/TLS version

By Crypto Suite



Generate Report

Includes flow details

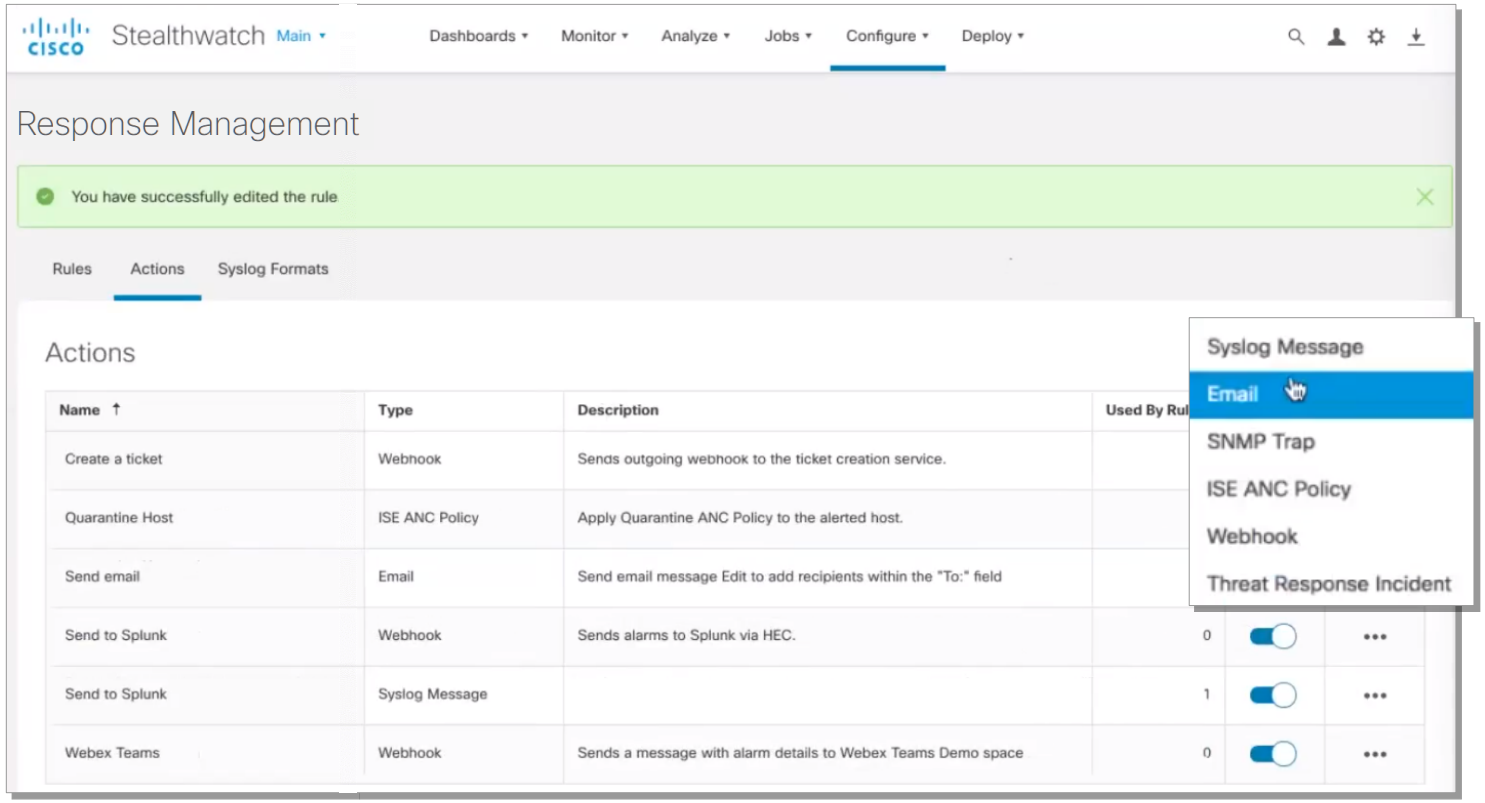
Relevant use cases:
- Using the ETA Cryptographic Audit Application
- Detecting Obsolete Encryption Protocols
- Using Encryption Auditing

Demo

Scalable visibility and security analytics

Automate Response and Alert Sharing

- Use webhooks to enhance data-sharing with third-party tools adding unparalleled flexibility in response management
- Send malware detections to SecureX threat response furthering forensic investigations
- Limit an endpoint's network access as detections occur combining Adaptive Network Control (ANC) and Cisco ISE.



Fully Automated Responses

Identity Services Engine

SecureX

servicenow

SIEMs

Cisco SecureX threat response

Email, Firewall, Endpoint, Umbrella, Secure Network Analytics

Cisco security products and threat Intel context

Other existing 3rd party products and threat Intel context

SecureX threat response

Detect

Enrichment and response

Investigate

Remediate

Integrates with Cisco, 3rd party products and threat intel

Incorporates threat intel

Centralized portal for investigation, detection and response

Architecture, components & management

Walk through the Secure Network Analytics enterprise architecture for on-premises deployment

Deeper dive into the Secure Network Analytics solution components

Centralized device management simplifies large enterprise deployment

Flexible deployment offers to get visibility everywhere

Secure Network Analytics
(Stealthwatch Enterprise)

Secure Network Analytics SaaS
(Stealthwatch Cloud PNM)

Secure Cloud Analytics
(Stealthwatch Cloud PCM)

On-premises data storage, granular tuning, SecOpsand NetOps use cases, air-gapped networks	Simple deployment, automated tuning, SecOps and light NetOps use cases	Suitable for all organizations using public cloud infrastructure like AWS, Azure, GCP and serverless environments
Hardware or virtual appliance	SaaS based network monitoring (including Meraki, container)	SaaS based
Priced by FPS (flows per second)	Endpoint-based pricing	Usage-based pricing determined by volume of log data

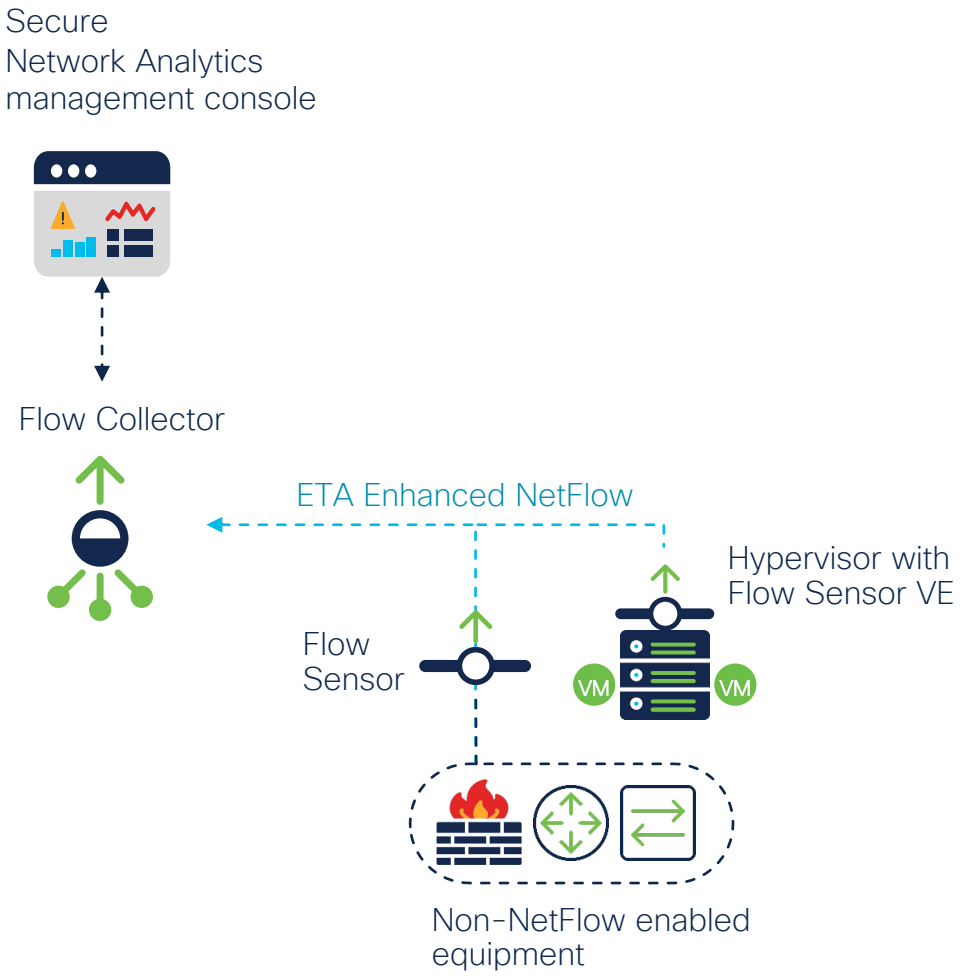
Flow sensor

Virtual or physical appliance that produces telemetry for network infrastructure incapable of generate NetFlow natively

Provides additional security context to enhance Secure Network Analytics security analytics

Additional information gathered

- ETA enhanced NetFlow
- Layer 7 application data
- URL information for web traffic
- TCP and ICMP flag details
- RTT (Round trip time)
- SRT (Server response time)
- Retransmissions
- X-Forwarded headers from web load balancers



Secure Network Analytics components

SMC

SMC VE (Virtual Edition)
SMC 2210

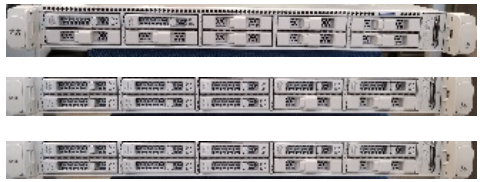
- SMC for Management and Configuration supports:
- Up to 25 Flow Collectors
- 10000 Network Access User sessions
- 15 concurrent managing users
- Scale up to 6 Million FPS in one deployment

Flow Collector

Flow Collector VE
FC 4210/FC5210

- Flow Collector is the center of Data Collection and Analytics.
- Up to 25 FC per deployment
- Up to 240 000 FPS per FC
- Up to 6TB of Flow Storage
- Up to 1Million Host Classified
- Up to 4000 Data Source per FC

Flow Sensor



Flow Sensor VE
FS1210/FS 3210/FS4210

- Ingest SPAN to generate telemetry and contextual data.
- Up to 20Gbps per FS, Copper and Fiber supported interface,
- 1Gb and 10Gb monitor interfaces

UDP director

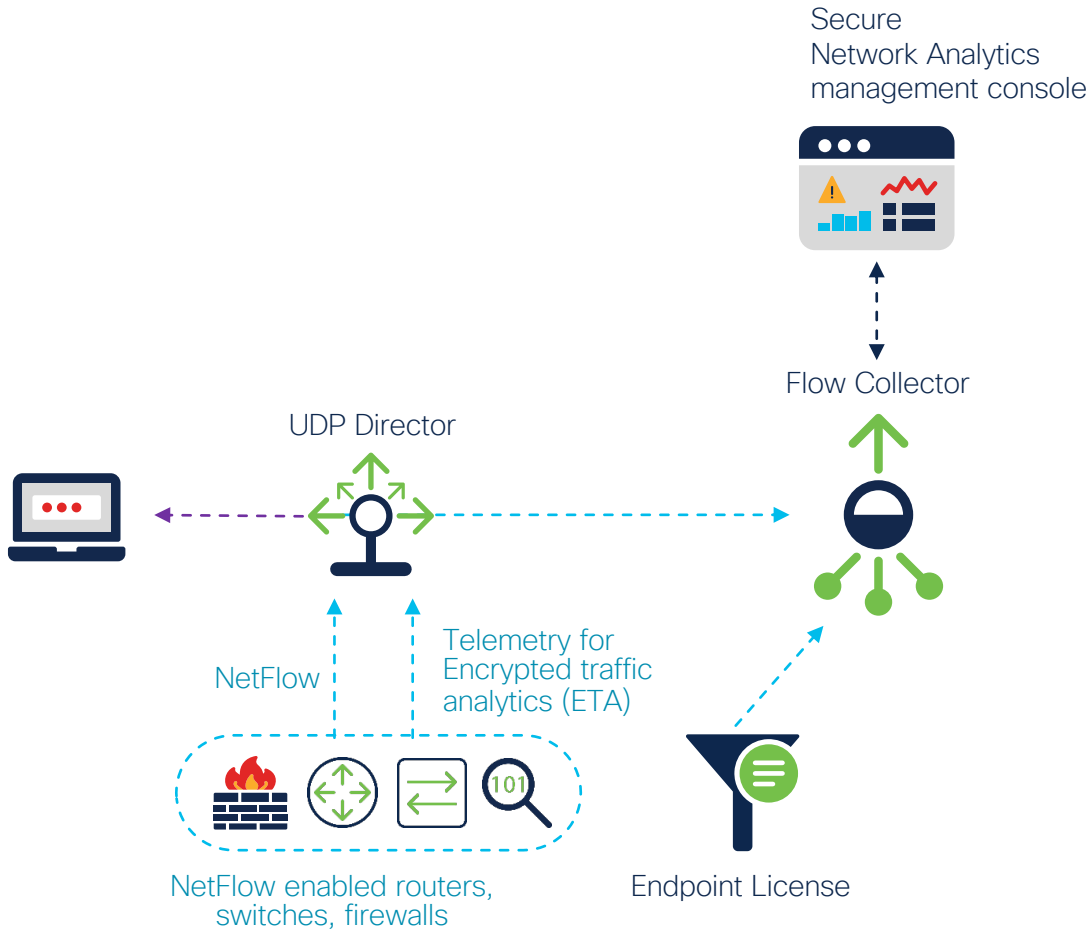
UDP Director VE (Virtual edition)
UDPD 2210

Replicates UDP traffic and generates NetFlow from SPAN traffic supporting:

- 1Gbps/10Gbps interfaces
- Up to 150,000 pps

Allows NetFlow, SYSLOG and SNMP data to be sent transparently to multiple collection points

Provides additional flexibility and ease of deployment

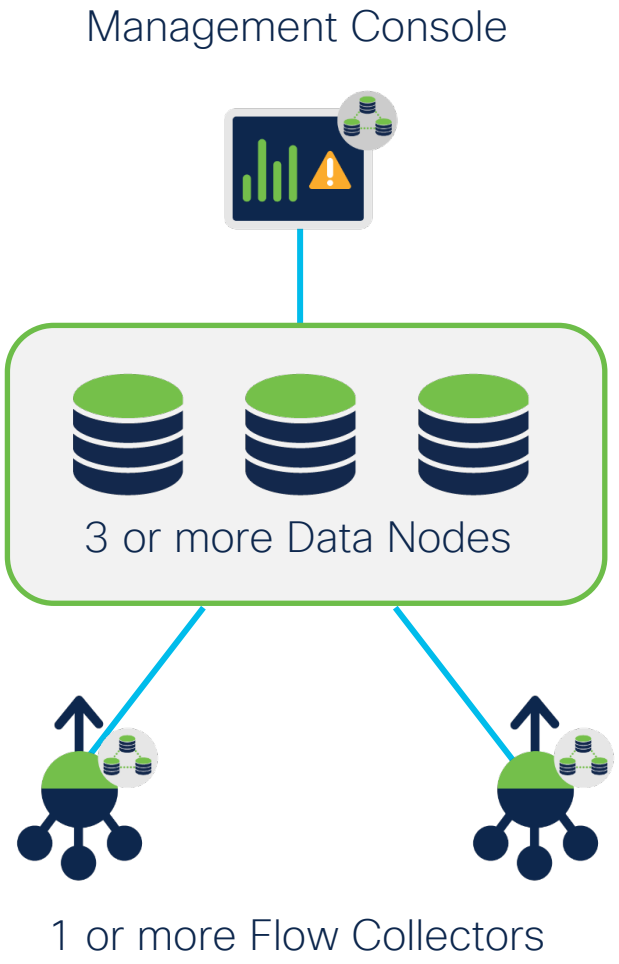


Introducing the Secure Network Analytics Data Store

- Scalable and long-term telemetry storage capabilities with no need to add additional Flow Collectors
- Enterprise class data resiliency
- Significantly improved query performance

What is the Secure Network Analytics Data Store?

- The Data Store is a new and improved database architecture design for Secure Network Analytics
- Each individual Data Store appliance will include a 3-Node database cluster
- Flow ingest by Flow Collectors is separated from data storage
- This distributed design enables scalable and resilient data storage, providing retention times of over a year
- Queries are handled by the Data Store, effectively increasing performance across all metrics by a significant magnitude



Integrations

Integrations: Secure Network Analytics integration with Cisco networking infrastructure

Data: Handling export data and alarms out of Secure Network Analytics

Secure Network Analytics integrations

Proxy
Web APP, web URL and user info

DNA Center
Automated setup and deployment

AnyConnect
Process and endpoint visibility

Identity Services Engine
User identity, device identity, mitigation and response

Secure
Network Analytics

External lookup
Extended analytics, threat investigation

SecureX threat response
Threat hunting and response

PAN
Application and user identity

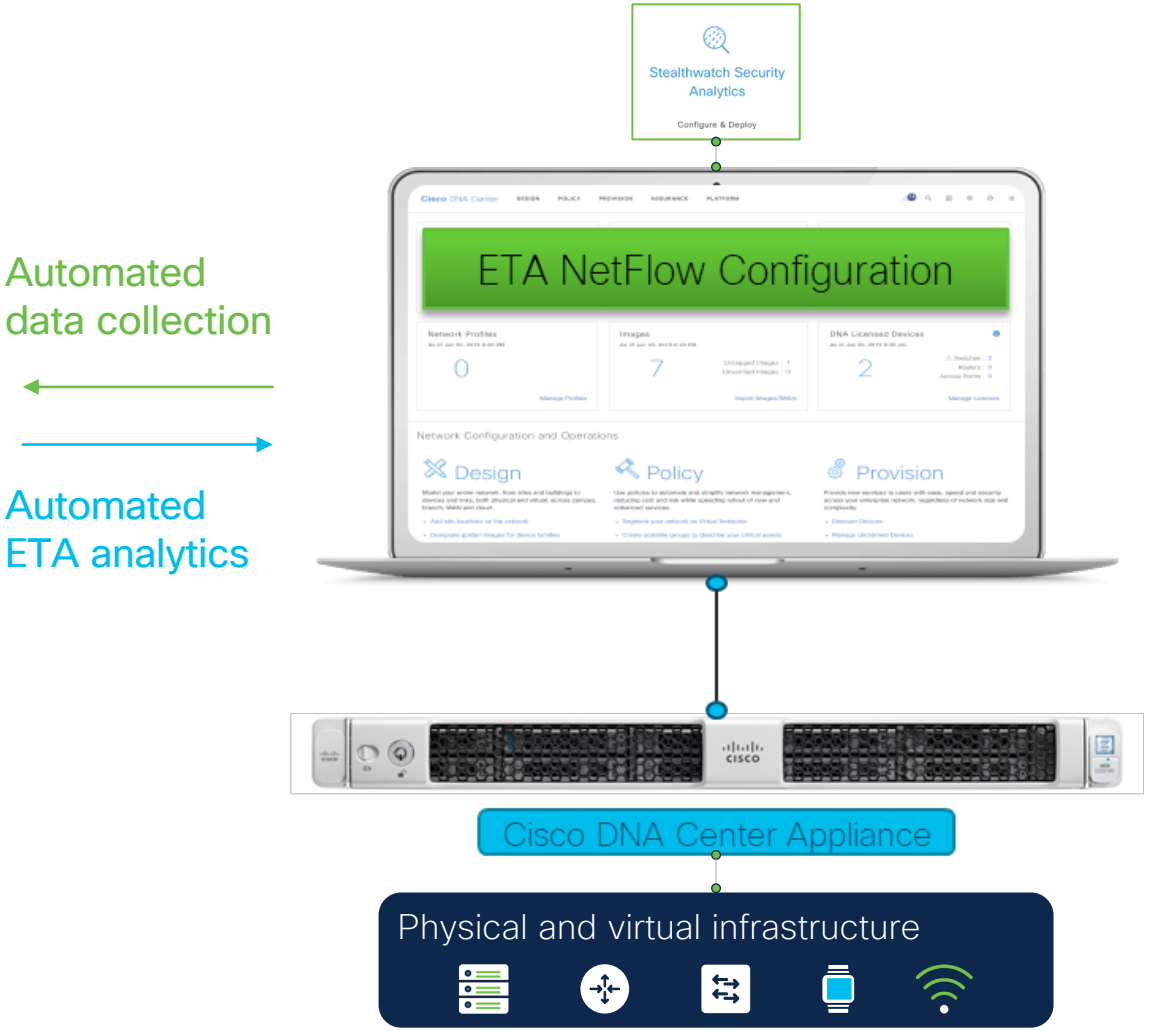
API
Automated and customized configuration and reporting

Security analytics integration with Cisco DNA Center

Secure Network Analytics app

Deploy ETA in minutes!

- Guided workflow makes it easier for networking teams to enable Secure Network Analytics within the enterprise
- Site based provisioning
  - Traditional wired networks
  - SD-access fabrics
- Automated readiness check
- Visibility of deployment status
- Security endpoint assurance



3rd party integration summary

Device	Integration type	Value
Checkpoint NGFW	v5/v9/IPFIX	NetFlow gen for visibility and NAT stitching
Barracuda NGFW	IPFIX	NetFlow gen for visibility
Gigamon	v5/v9/IPFIX	NetFlow generation from SPAN traffic
IXIA NVS	IPFIX	NetFlow gen for visibility
Palo Alto	IPFIX	Enriched NetFlow gen for visibility
TRIPWIRE	Web lookup	Correlation and investigation workflow
Ziften	Web lookup	Correlation and investigation workflow
Savvius	SYSLOG	Correlating events + trigger packet capture
Arcsight	SYSLOG	Correlating events from Secure Network Analytics