



Say hello  
to the future.

**Cisco Connect 2019**

Malaysia, Kuala Lumpur · 18 April 2019

#CiscoConnectMY



# Security and Visibility for the Modern Networks

*Ross Traynor, Cybersecurity Specialist, Cisco*

*Eric Rennie, Systems Engineer, Cybersecurity, Cisco*

# Digitization complicates visibility

Market demands have taken the network beyond your perimeter

## More IoT devices connect everyday

Over 20B connected "things" will be in use by 2020

## Users work anywhere across many devices

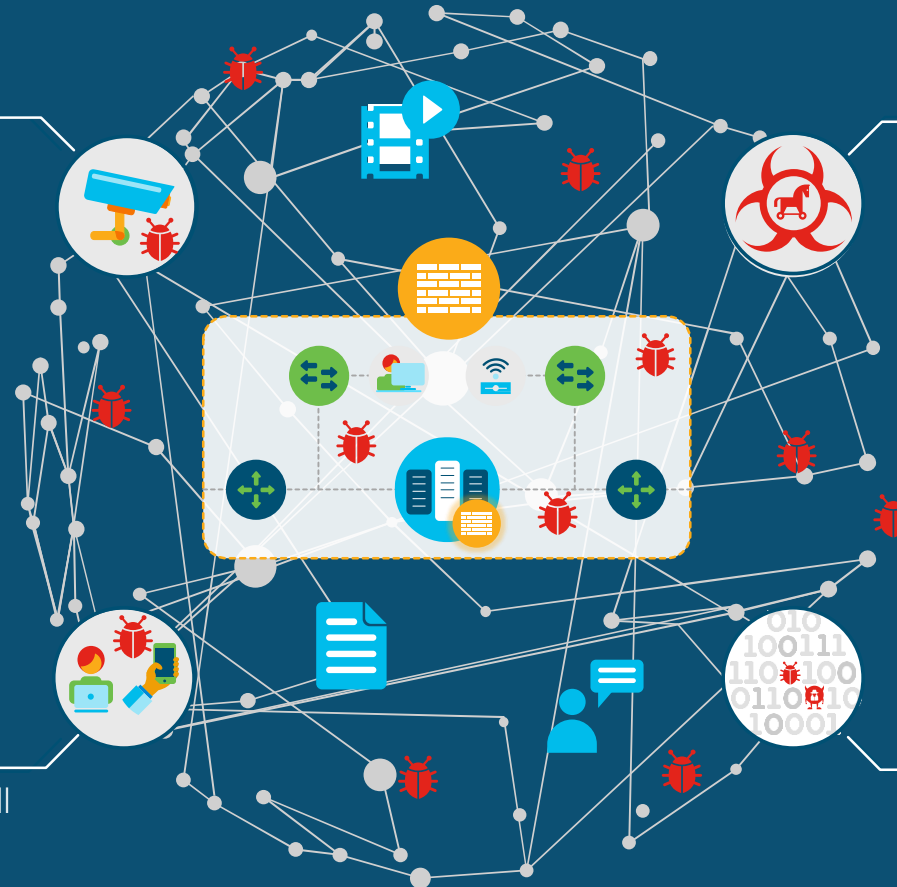
By 2020, 2/3<sup>rd</sup>s of all IP traffic will come from wireless and mobile devices

## Threats are more numerous and complex

Companies experienced a 27.4% average increase in security breaches in 2019

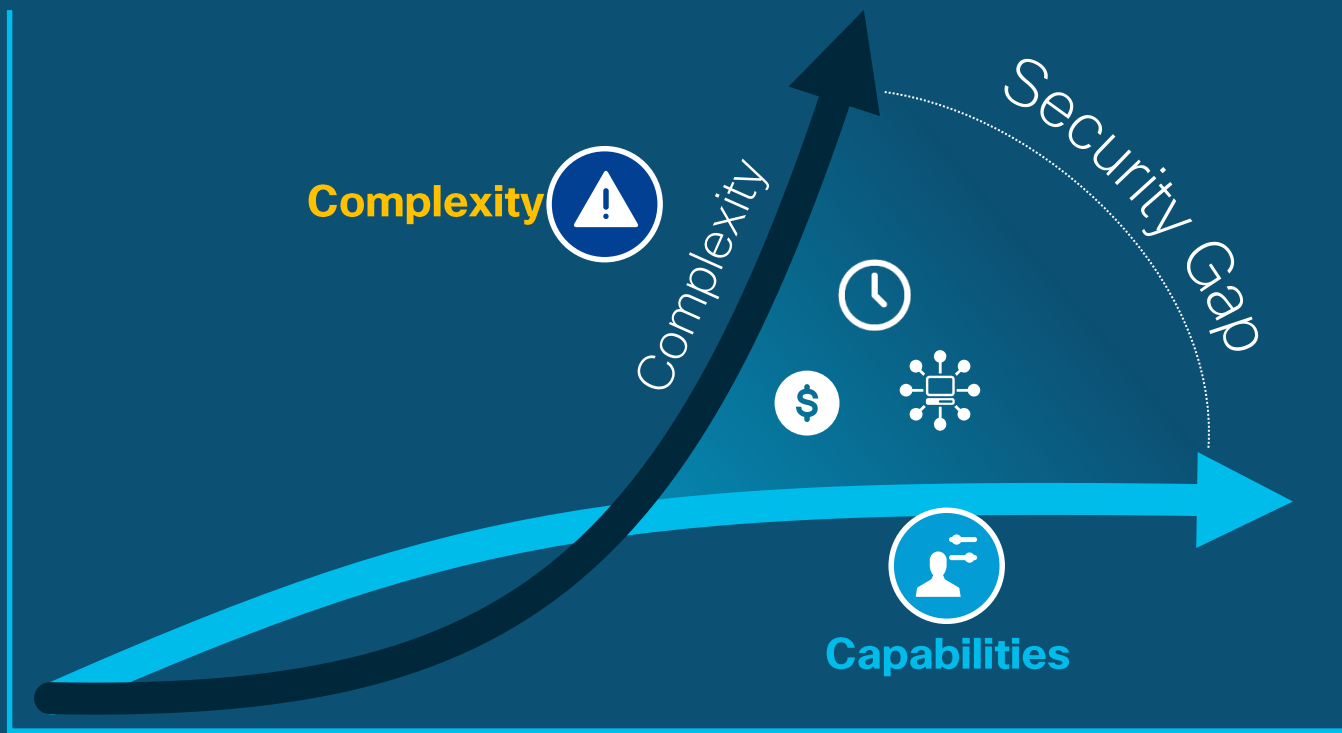
## Threats are using encryption to evade detection

3X increase in encrypted communication from malware in a 12-month period



# The vendor buffet is not a strategy

Adding point solutions adds complexity & can make you less secure



**55%** Of customers rely on more than 5 vendors to secure their network<sup>1</sup>

**54%** Of legitimate security alerts are not remediated due to lack of integrated defense systems<sup>2</sup>

**100 days** Industry average to detect a common threats<sup>3</sup>

<sup>1</sup> [Cisco 2019 Annual Cybersecurity Report](#)

<sup>2</sup> [Cisco 2019 Annual Cybersecurity Report](#)

<sup>3</sup> [Cisco 2019 Mid-Year Cybersecurity Report](#)

# The Solution: Network + Security

Activate your network for more holistic security

## Understand behavior

Identify host role and monitor behavior without endpoint agents



## See everything

Transform the network into a powerful security sensor for complete visibility



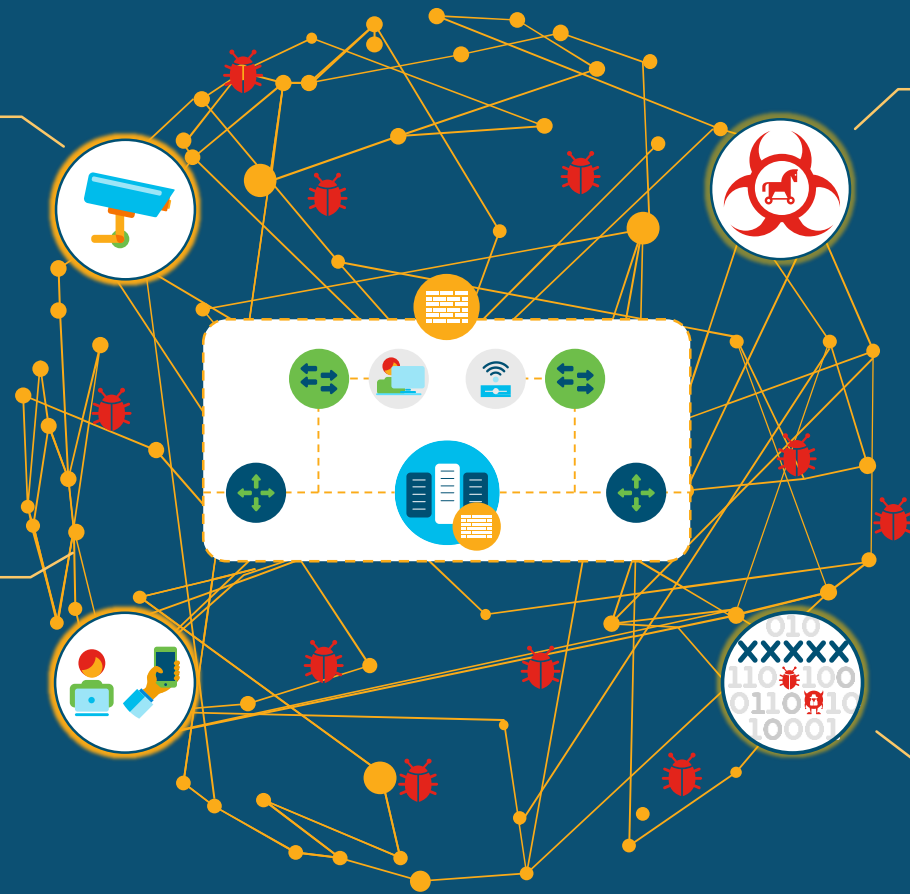
## Contain and isolate threats

Dynamically enforce software-defined segmentation based on business roles



## Detect encrypted threats

Use advanced analytics to automatically detect encrypted threats without decryption



# Cisco Stealthwatch

Gain confidence in your security effectiveness

## Contextual network-wide visibility



## Predictive threat analytics



## Automated detection and response



Using existing network infrastructure

# Stealthwatch Use Cases

## Context-Aware Visibility

- ❑ Network, application, and user activity
- ❑ Monitor lateral movement using the network as a sensor

## Threat Detection

- ❑ Advanced persistent threats
- ❑ Insider threat
- ❑ DDoS
- ❑ Data exfiltration

## Incident Response

- ❑ In-depth, flow-based forensic analysis of suspicious incidents
- ❑ Scalable repository of security information

## Network Planning & Diagnostics

- ❑ Network segmentation to profile application / device traffic
- ❑ Capacity planning
- ❑ Performance monitoring
- ❑ Application awareness

## User Monitoring

- ❑ Cisco ISE
- ❑ Monitor privileged access
- ❑ Policy enforcement

## Customer Use Cases:

<https://www.techvalidate.com/product-research/cisco-stealth-watch/facts>





# Key features

## Visibility everywhere

Analyses enterprise telemetry from any source (NetFlow, IPFIX, sFlow, other Layer 7 protocols) across the extended network

## Unique threat detection

Combination of multi-layer machine learning and behavioral modeling provides the ability to detect inside as well as outside threats

## Encrypted Traffic Analytics

Only product that can analyze encrypted traffic to detect malware and ensure policy compliance without decryption

## Smart segmentation

Create logical user groups that make sense for your business, monitor the effectiveness of segmentation policies through contextual alarms

## Rapid Threat Containment

Quarantine infected hosts easily using the Identity Services Engine (ISE) integration, collect and store network audit trails for deeper forensic investigations





# Collecting and optimizing telemetry



# Scaling and Optimization: stitching



Unidirectional  
Telemetry  
Records

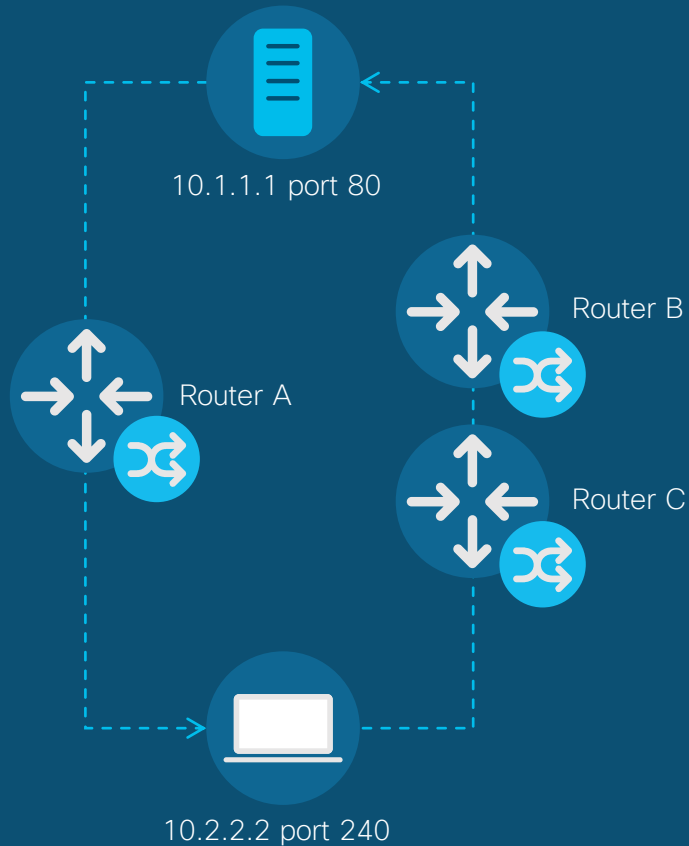
Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712

Bidirectional  
Telemetry Record

Conversation record  
Easy visualization and analysis

Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	Interfaces
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	eth0/1 eth0/2

# Scaling and Optimization: deduplication



Router A: 10.1.1.1:80 → 10.2.2.2:1024

Router B: 10.2.2.2:1024 → 10.1.1.1:80

Router C: 10.2.2.2:1024 → 10.1.1.1:80

Duplicates

## Deduplication

- Avoid false positives and misreported traffic volume
- Enable efficient storage of telemetry data
- Necessary for accurate host-level reporting
- No data is discarded



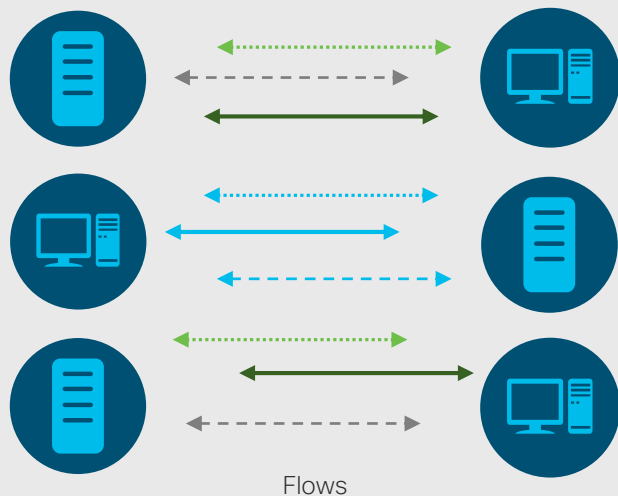
# Industry-leading Security Analytics



# Anomaly detection using behavioral modeling

## Collect and analyze telemetry

Comprehensive data set optimized to remove redundancies



## Create a baseline of normal behavior

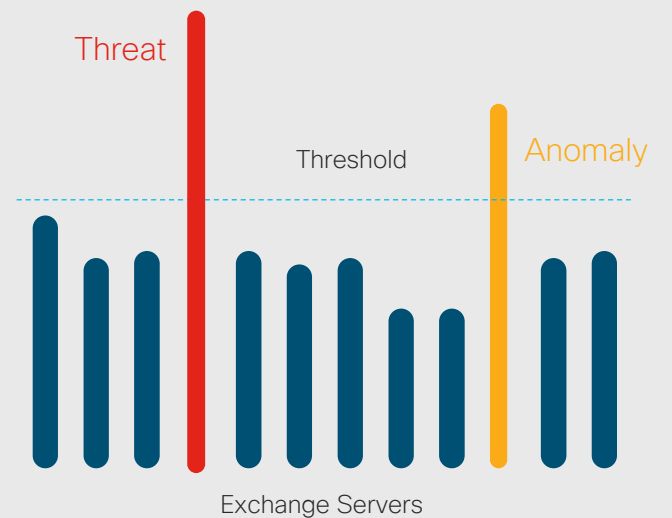
Security events to detect anomalies and known bad behavior

### Analysis of multiple threat behaviors

Number of concurrent flows	New flows created	Number of SYNs received
Packet per second	Number of SYNs sent	Rate of connection resets
Bits per second	Time of day	Duration of the flow

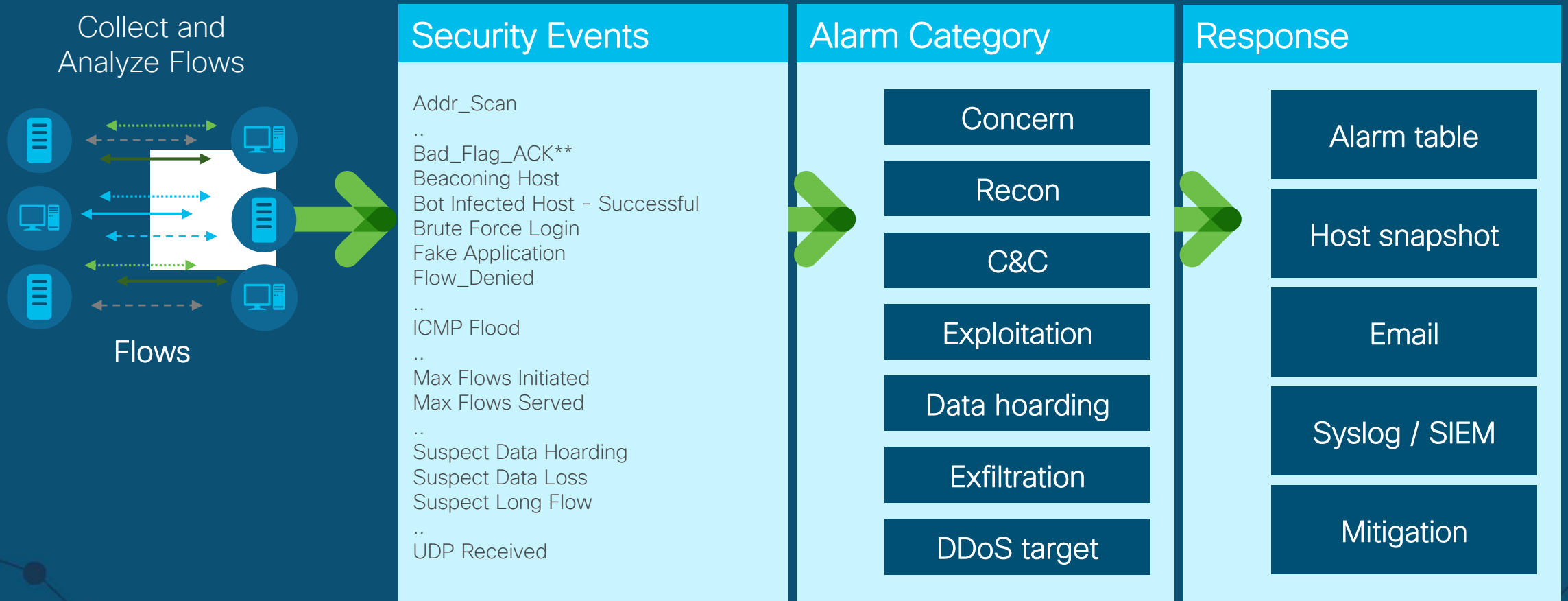
## Alarm on anomalies and behavioral changes

Alarm categories for high-risk, low-noise alerts for faster response



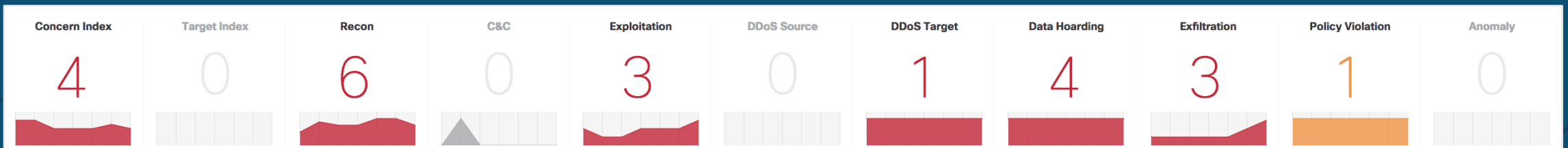
# Behavioral & Anomaly Detection Model

Behavioral Algorithms are Applied to Build “Security Events”



# Logical alarms based on suspicious events

Source or target of malicious behavior	Reconnaissance	Command and Control	DDoS Activity	Insider threats
Scanning, excessive network activity such as file copying or transfer, policy violation, etc.	Port scanning for vulnerabilities or running services	Communication back to an external remote controlling server through malware	Sending or receiving SYN flood and other types of data floods	Data hoarding and data exfiltration



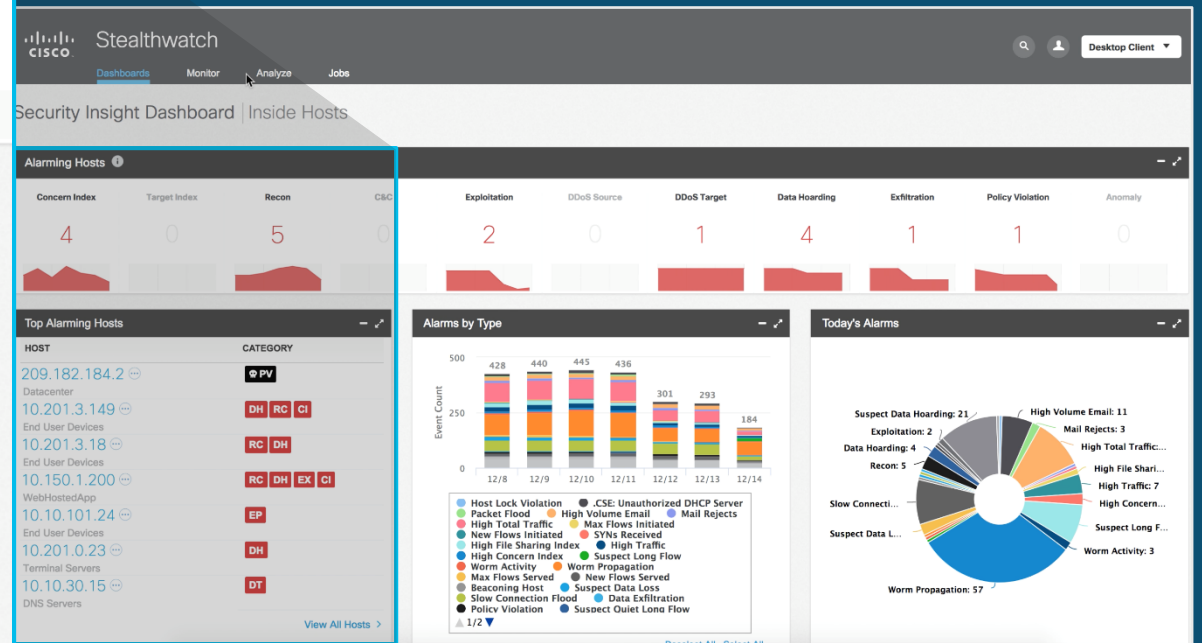
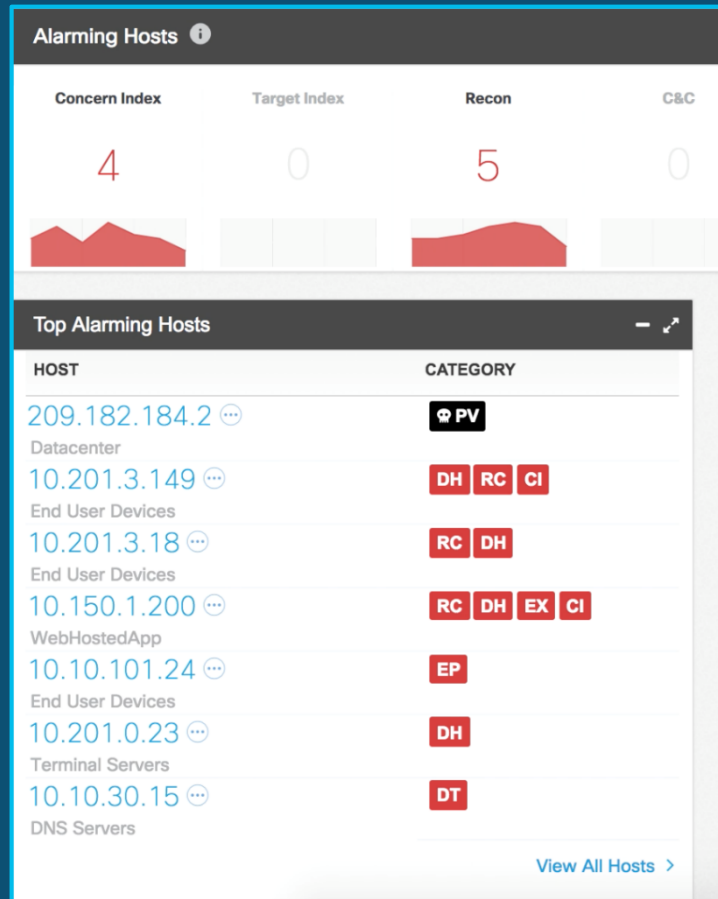


# Alarms tied to specific entities

Quick snapshot of malicious activity


Suspicious behavior linked to logical alarms

Risks prioritized to take immediate action



# Investigating a host

### Host Summary



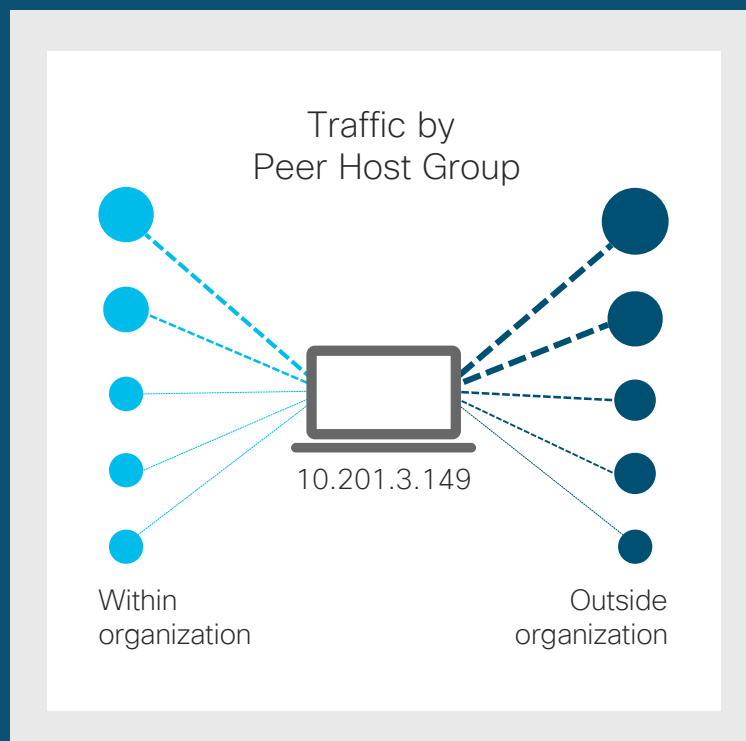
Flows History

User Name: \_\_\_\_\_  
Device Name: \_\_\_\_\_  
Device Type: \_\_\_\_\_  
Host Group: \_\_\_\_\_  
Location: \_\_\_\_\_  
Last Active Status: \_\_\_\_\_  
Session Information: \_\_\_\_\_  
Policies: \_\_\_\_\_

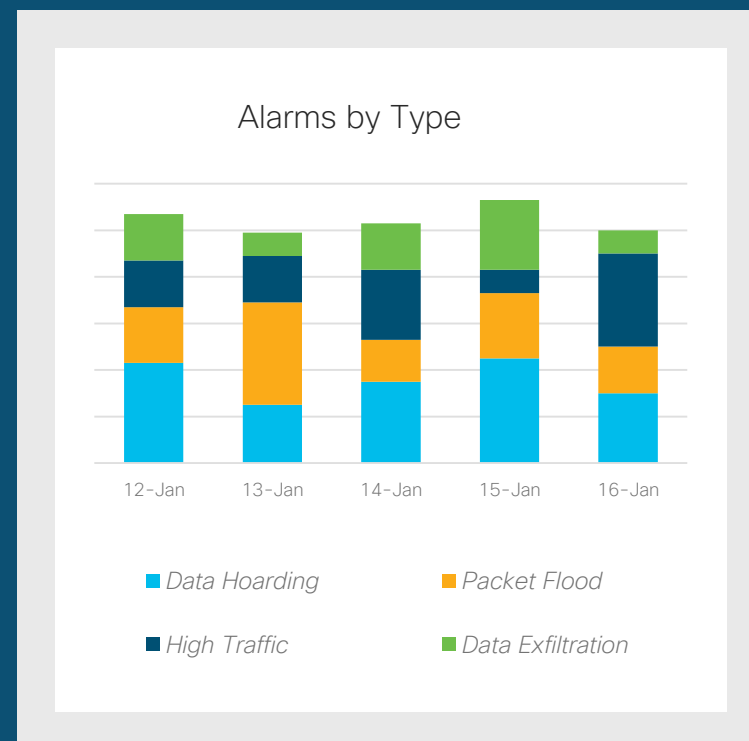
Quarantine Unquarantine

The Host Summary panel displays a central laptop icon and a progress bar. Below these are two tabs: 'Flows' and 'History'. A series of labels with corresponding input fields are listed: 'User Name', 'Device Name', 'Device Type', 'Host Group', 'Location', 'Last Active Status', 'Session Information', and 'Policies'. At the bottom, there are two buttons: 'Quarantine' and 'Unquarantine'.

Summary of aggregated host information



Observed communication patterns



Historical alarming behavior

A network diagram is visible in the top right and bottom left corners of the slide. It consists of several nodes (represented by small circles) connected by thin white lines. The nodes are colored in shades of orange, green, and grey. The connections form a complex web of lines across the dark blue background.

# Encrypted Traffic Analytics

# Encrypted Traffic Analytics (ETA)

Visibility and malware detection with decryption



## Malware in Encrypted Traffic

Is the payload within the TLS session malicious?

- End to end confidentiality
- Channel integrity during inspection
- Adapts with encryption standards

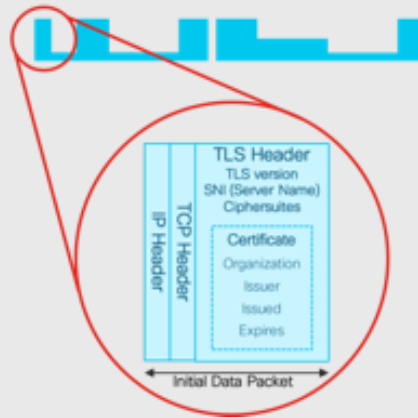
## Cryptographic compliance

How much of my digital business uses strong encryption?

- Audit for TLS policy violations
- Passive detection of Ciphersuite vulnerabilities
- Continuous monitoring of network opacity

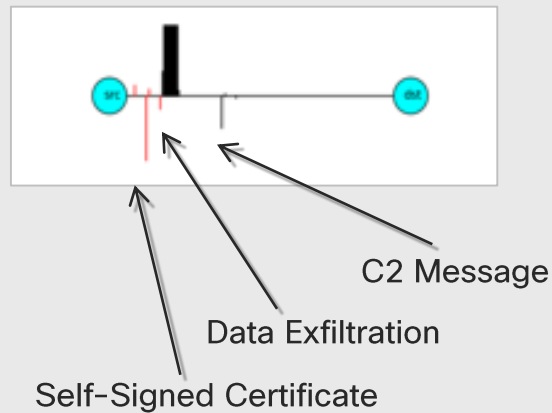
# Detect malware in encrypted traffic

Initial data packet



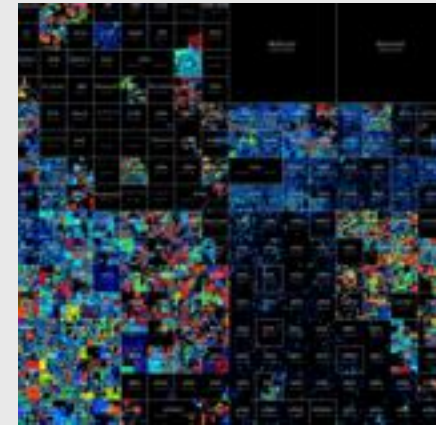
Make the most of the unencrypted fields

Sequence of packet lengths and times



Identify the content type through the size and timing of packets

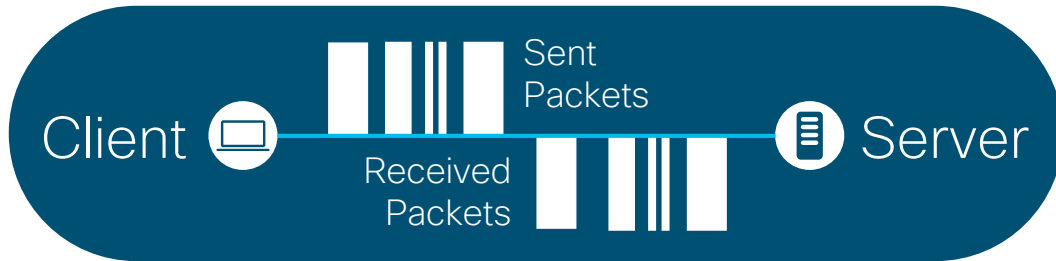
Global Risk Map



Know who's who of the Internet's dark side

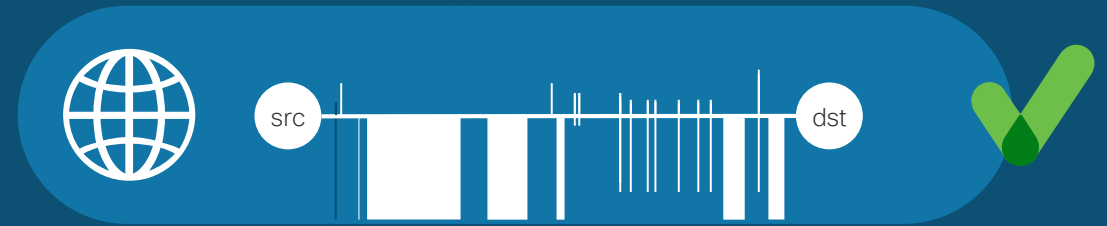
# Identifying malicious encrypted traffic

Model

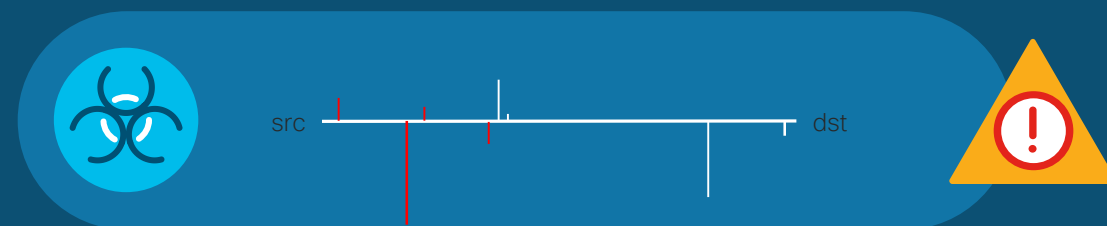


Packet lengths, arrival times and durations tend to be inherently different for malware than benign traffic

Google Search Page Download



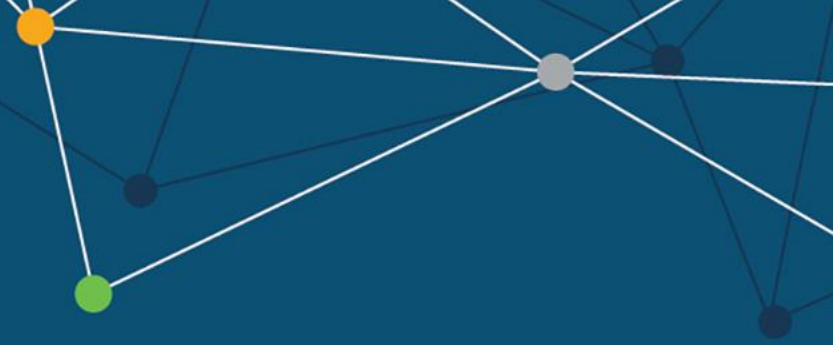
Initiate Command and Control



Exfiltration and Keylogging



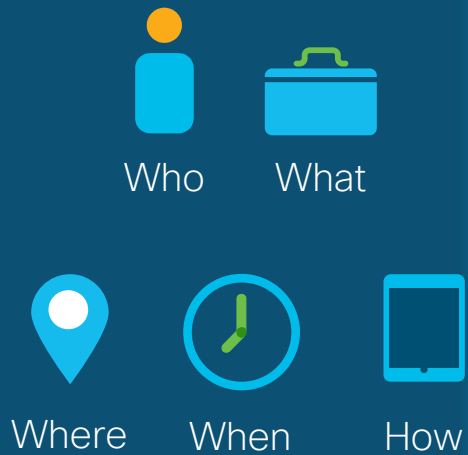
# Accelerated Threat Response





# Cisco Identity Services Engine (ISE)

Network and User Context



Identity Services Engine

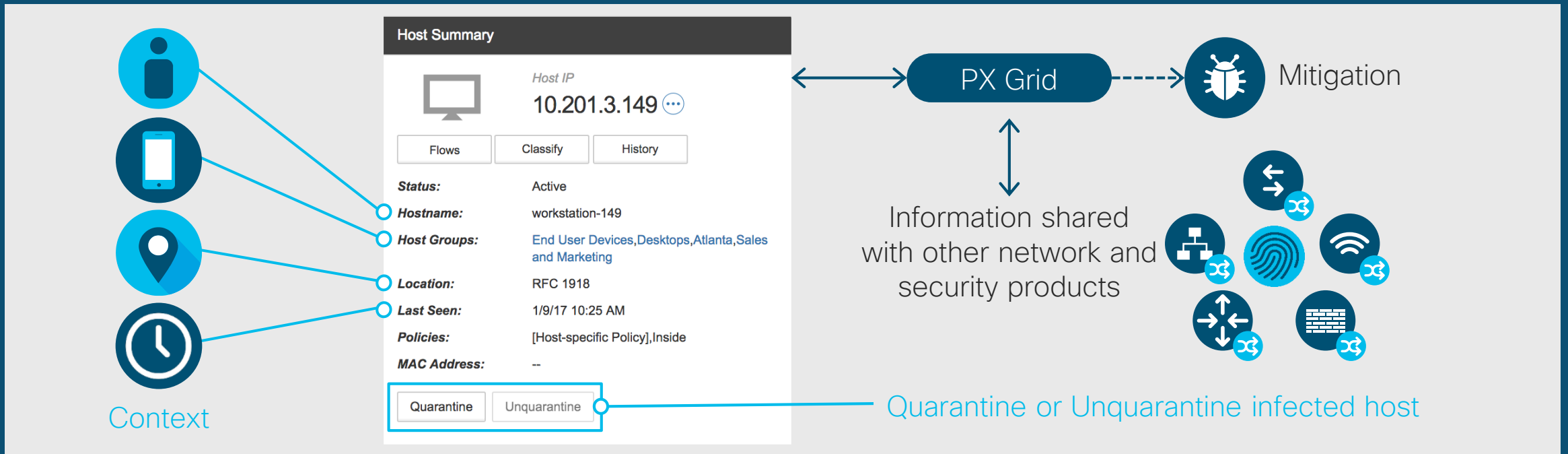
Stealthwatch Security Analytics



**Send contextual data collected from users, devices, and network to Stealthwatch Enterprise for advanced insight**

# Rapid Threat Containment

Without any business disruption



Cisco®  
Identity Services Engine



Stealthwatch  
Management Console

A network diagram with nodes and lines is visible in the top right and bottom left corners of the slide. The top right diagram features a central grey node connected to several other nodes, including one orange, one green, and several black nodes. The bottom left diagram shows a few black nodes connected by lines.

# Stealthwatch Enterprise Architecture and integrations

# Required core components

## Stealthwatch Management Console (SMC)

- A physical or virtual appliance that aggregates, organizes, and presents analysis from Flow Collectors, Identity Services Engine (ISE), and other sources
- User interface to Stealthwatch
- Maximum 2 per deployment

## Flow Collector (FC)

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

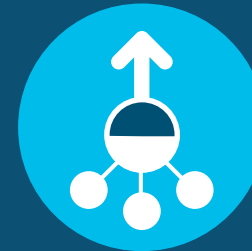
## Flow Rate License

- Collection, management, and analysis of telemetry by Stealthwatch Enterprise
- The Flow Rate License is simply determined by the number/type of switches, routers, firewalls and probes present on the network

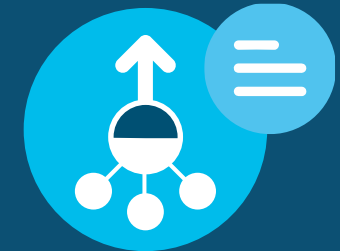
Management Console



Flow Collector

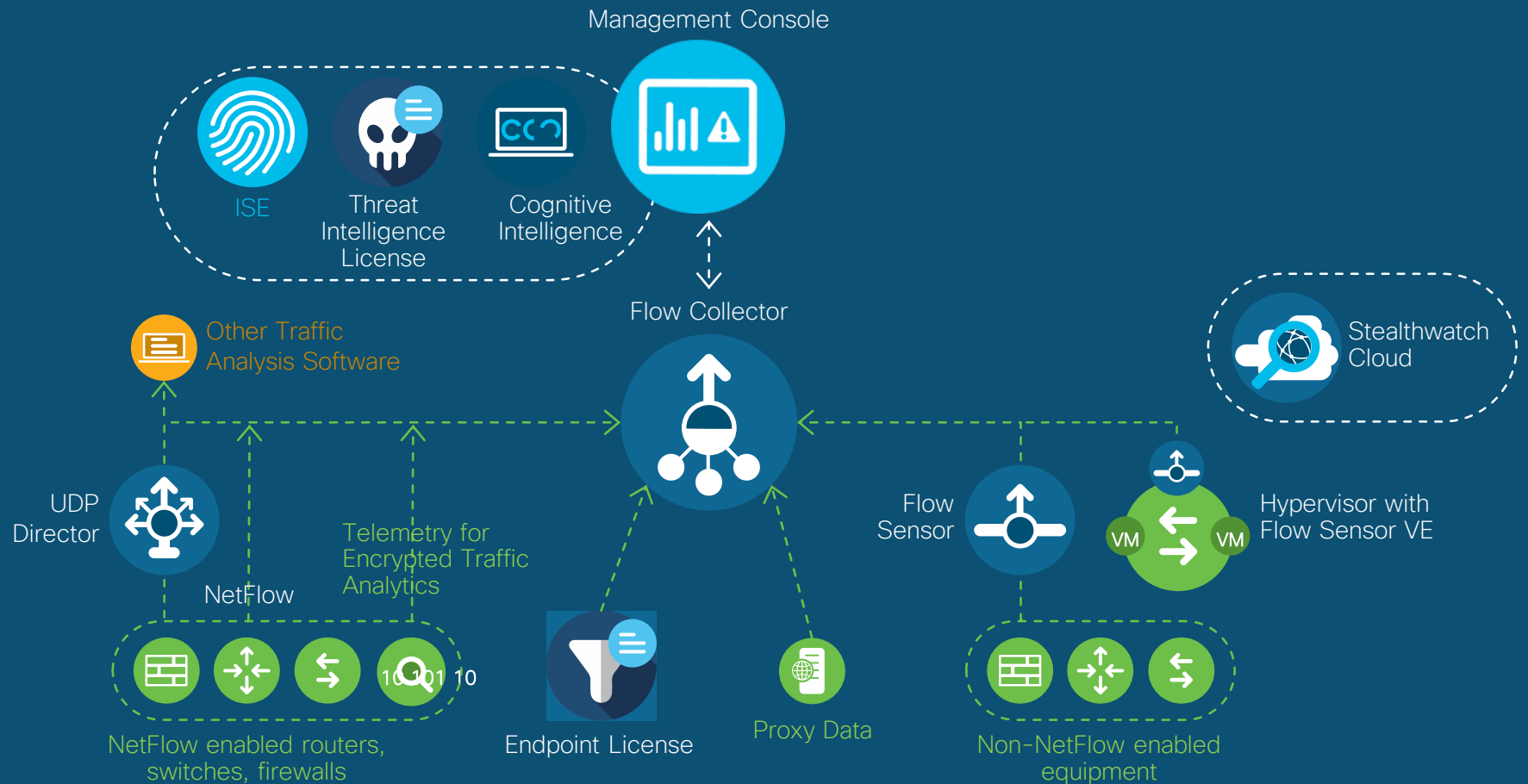


Flow Rate License

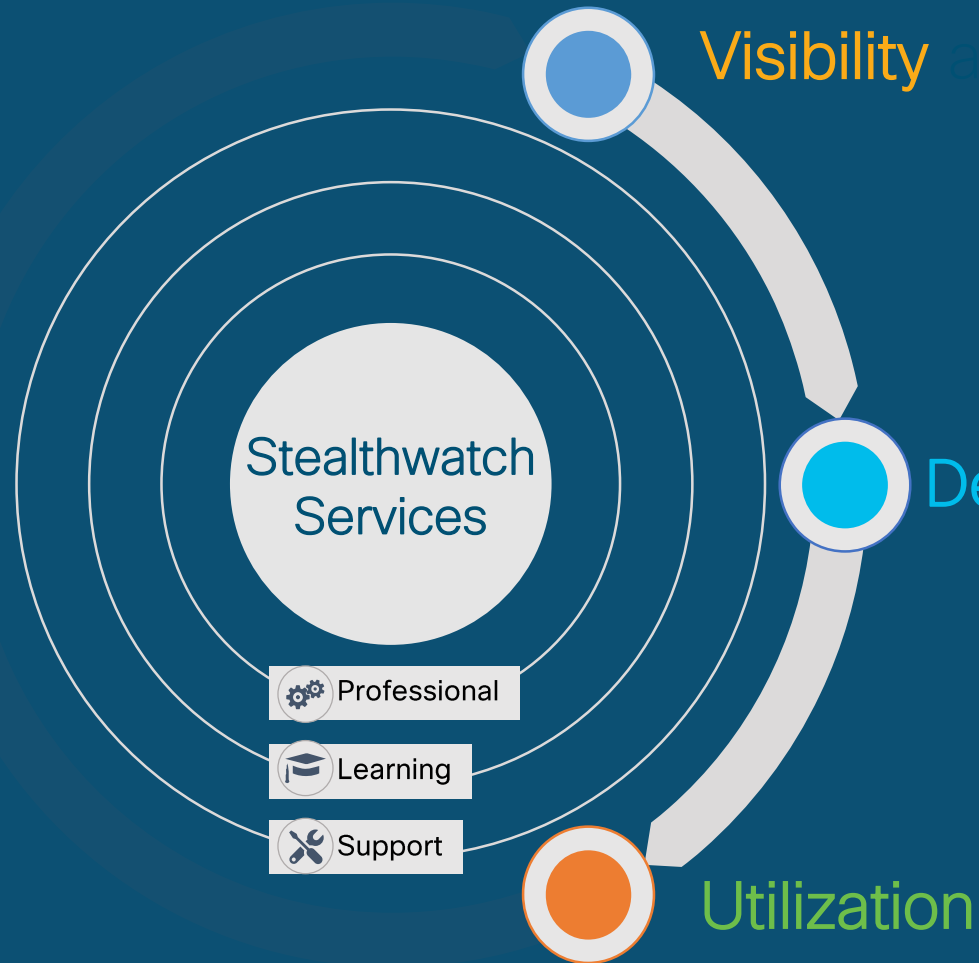


# Stealthwatch Enterprise architecture

Comprehensive  
visibility and  
security analytics



# Solution lifecycle for Cisco Stealthwatch Enterprise and Stealthwatch Customer Experience



across your entire network

- ✓ Error free deployment
- ✓ Highest performance flow collection
- ✓ Train your staff
- ✓ 24x7 Customer Support

based on your business needs

- ✓ Adopt and improve threats detection fidelity
- ✓ Reduce time to detection and response of threats
- ✓ Tactical workshops for use cases

- ✓ Integrate with your incident response plan
- ✓ Integrate with your telemetry stack
- ✓ Virtual labs and e-learning courses
- ✓ 24x7 Customer Support

# How Stealthwatch CX has helped

Provide network visibility across IT network



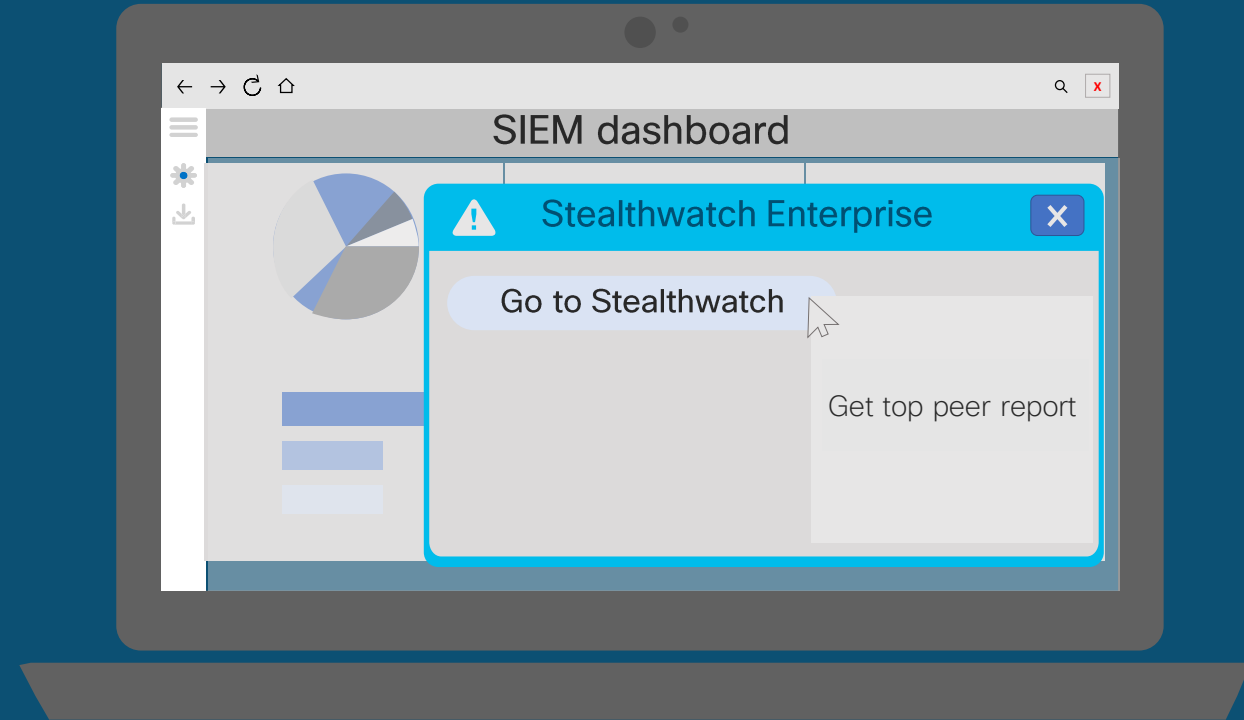
## Challenges

- SIEM integration with Stealthwatch Enterprise is extremely difficult to do on your own
- Many SOC teams place strong emphasis on working out of a SIEM
- SIEM is viewed as the “single pane of glass” for their security workflow



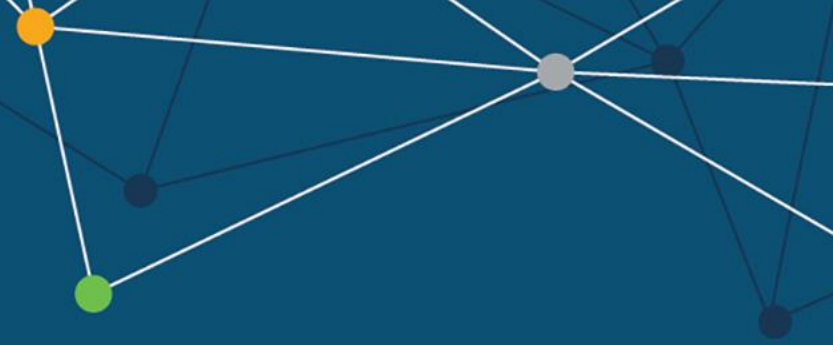
## Results

- Through an extended set of REST API capabilities that are installed for the customer, Professional Services works directly with the customer to understand their investigation workflow
- Integrate these API capabilities into their SIEM through either apps, add-ons, or right-click pivot capabilities
- Reduce the mean time to resolution for customers by enriching the data they use for investigation with Cisco Stealthwatch data
- Provide a clearer picture as to the nature and behaviour of the suspicious host in question, giving them a higher degree of accuracy in securing their networks faster.





Demo





Say hello  
to the future.

**Cisco Connect 2019**

Malaysia, Kuala Lumpur · 18 April 2019

#CiscoConnectMY