cisco Secure

Cisco Secure Network Analytics Customer Test Drive

Learn how to turn your network into a sensor and enforcer using behavioral analytics and machine learning

Updated Jun 2021

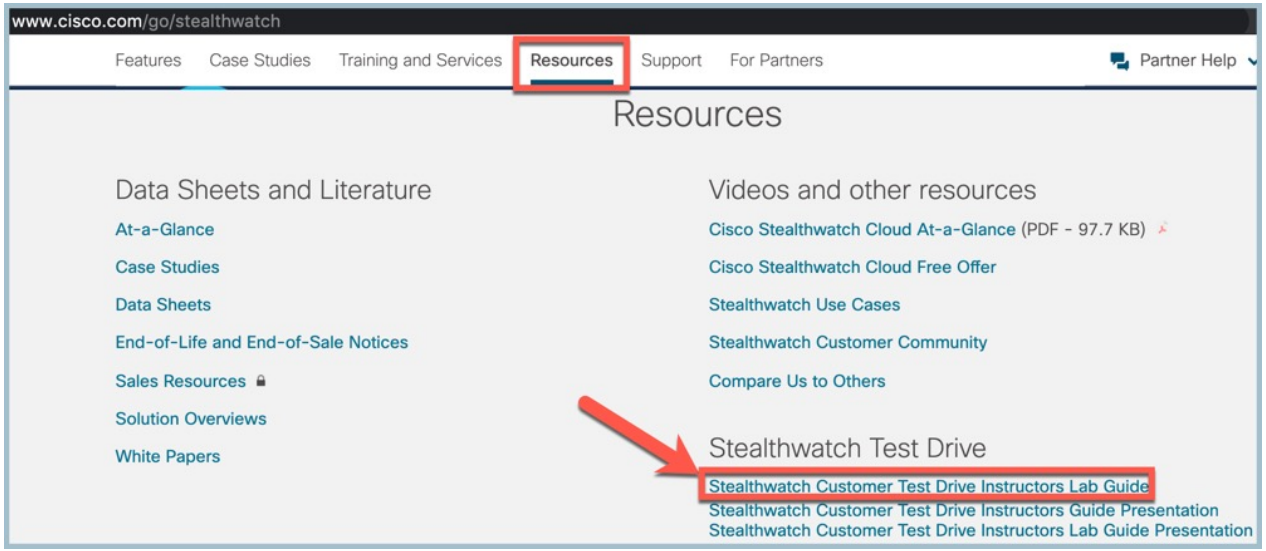
Agenda

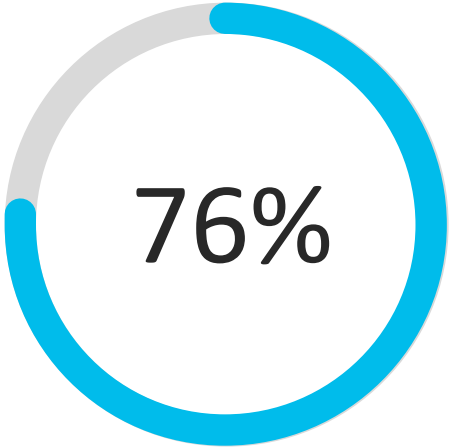
Hands on labs

1. Overview and Lab Setup
2. Breach Detection Labs
3. Insider & Advanced Threat Detection Labs
4. High Risk Application Detection Labs
5. Policy Violation Labs
6. Encrypted Traffic Analytics
7. Public Cloud Monitoring

Lab Guide Download

www.cisco.com/go/stealthwatch





IT professionals say that *lack of visibility* is their biggest challenge in addressing network threats

– The Ponemon Institute

Effective security depends on total visibility

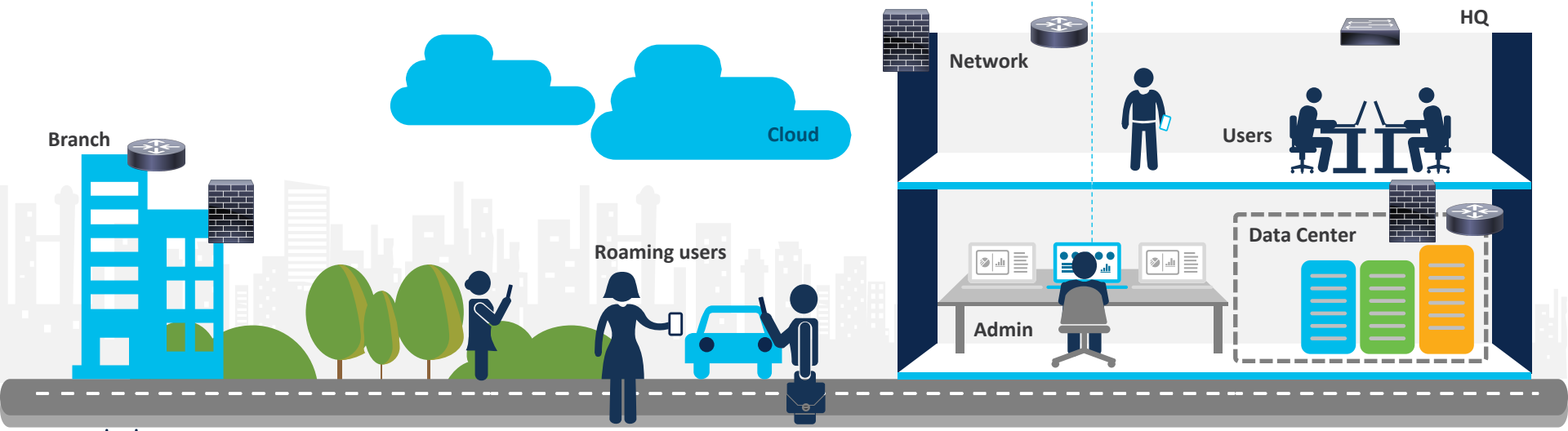
KNOW every host

RECORD every conversation

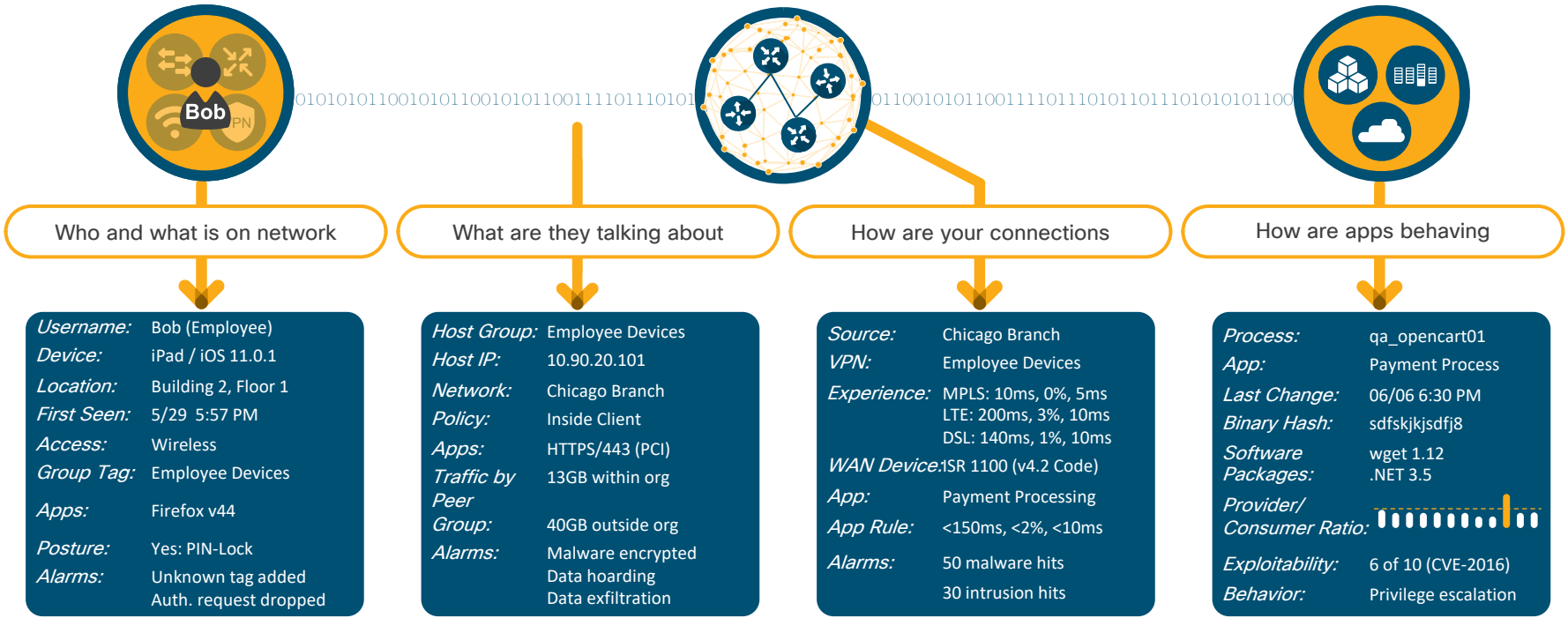
Understand what is **NORMAL**

Be alerted to **CHANGE**

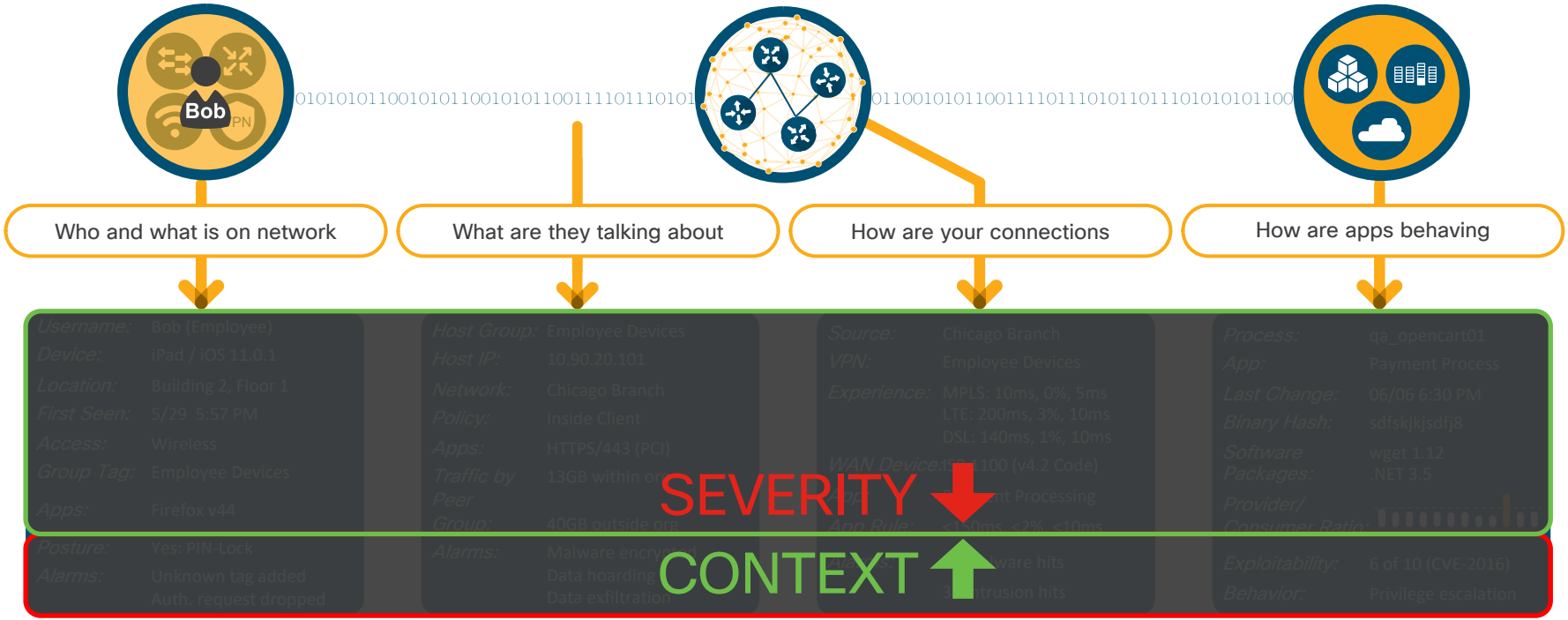
Respond to **THREATS** quickly



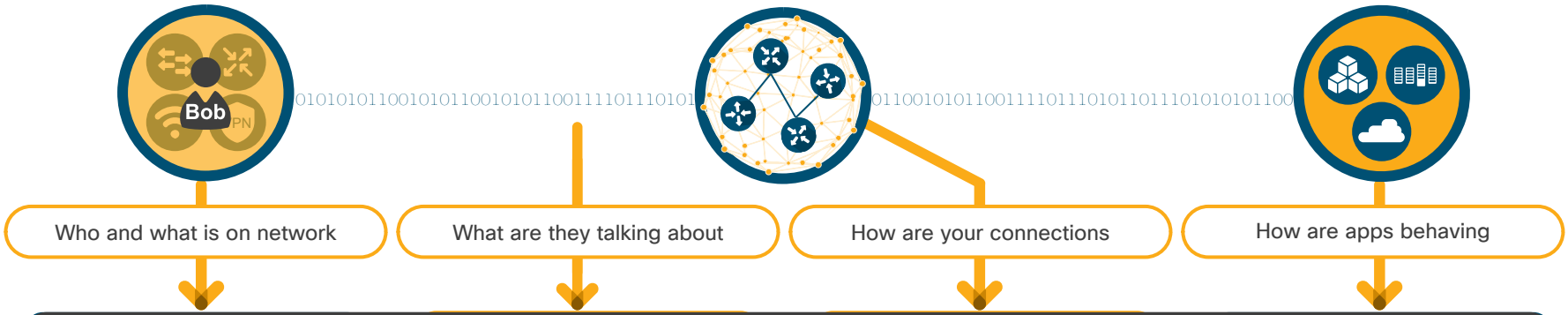
Continuous visibility correlated from user to process



Continuous visibility correlated from user to process



Continuous visibility correlated from user to process



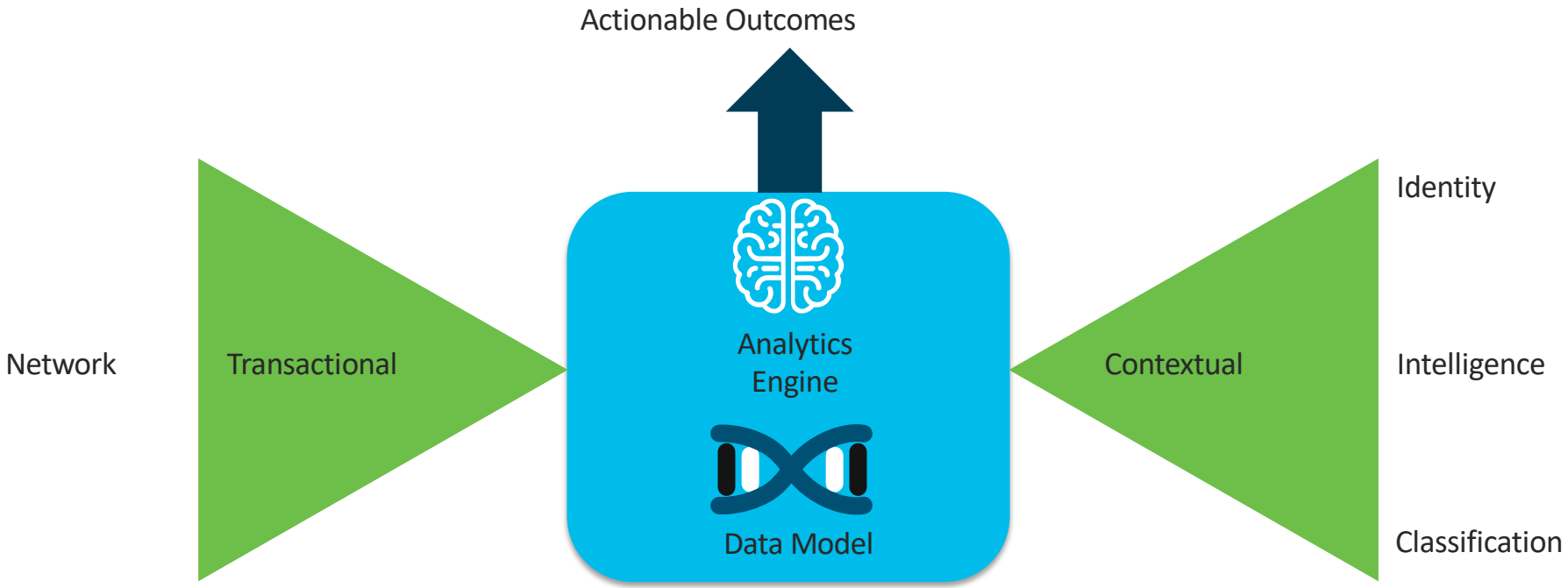
Bob on employee device didn't authenticate

Employee device in Chicago sending malicious encrypted traffic & hoarding/leaking data

Chicago connection to payment process experienced many malware & intrusion hits

Payment process is running exploitable software and escalated privileges for Bob

Secure Network Analytics in a Nutshell

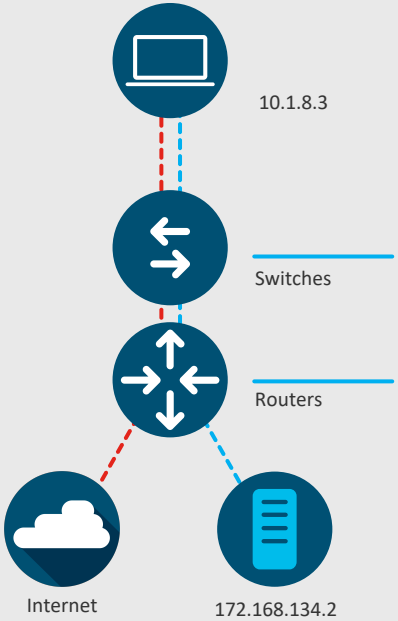


Cisco Secure Network Analytics: Is a collector and aggregator of network telemetry for the purposes of data modelling, security analysis and monitoring.

The network is a valuable data source

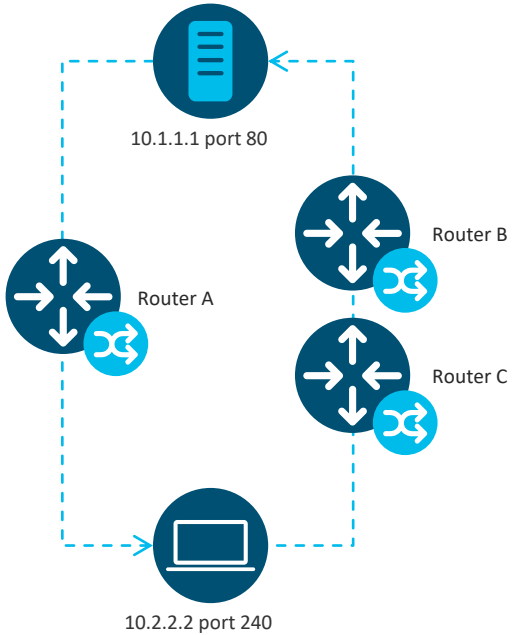
What it provides:

- A trace of every conversation in your network
- Network usage metrics
- Ability to view north-south as well as east-west communication
- 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

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

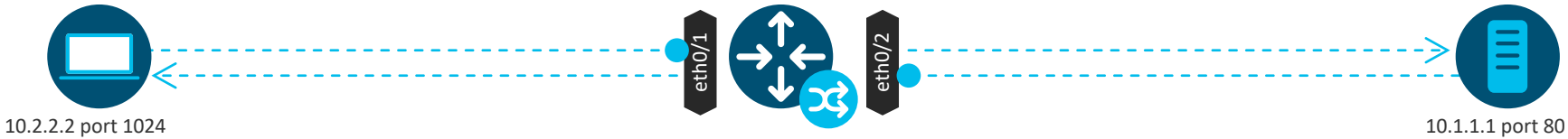
Router C: 10.2.2.2:1024 → 10.1.1.1:80

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

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

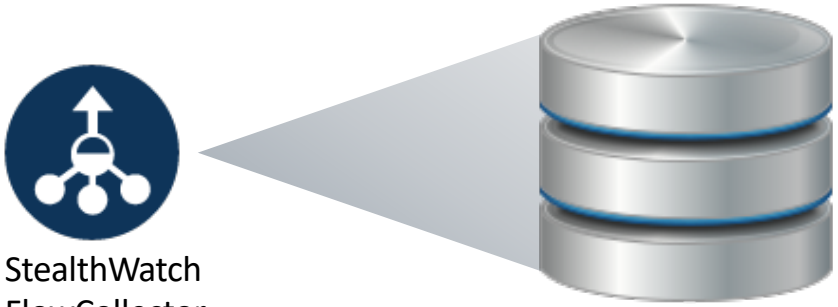
Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	Interfaces
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	eth0/1 eth0/2

Conversation record

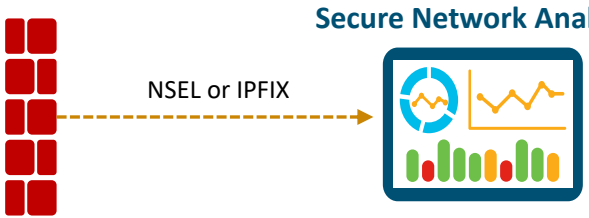
Easy visualization and analysis

Storage

- Secure Network Analytics has the ability to store flows for long period of time
  - On average 6 to 8 months
- Stored on a hardened Linux OS in a Vertica Database
  - Use Case: Cisco CSIRT Team



End to End Visibility Through NAT Gateway



- End to End visibility
- Know who is behind a shared public IP

START	SUBJECT IP A...	SUBJECT NAT	SUBJECT NAT HOSTNAME	SUBJECT NAT PORT	SUBJECT PORT...	PEER IP ADDRE...	PEER PORT/PR...	ACTIONS
Ex. 06/09/201	Ex. 10.10.10.1	Ex. 50.233.88.6	Ex. cisco	Ex. 57100	Ex. 57100/UDP	Ex. 10.255.255.:	Ex. 2055/UDP	
Jul 9, 2019 3:33:33 PM (8min 43s ago)	10.201.0.16	209.182.184.2	spyglass.lancope.com	9428	56420/UDP	221.7.138.5	53/UDP	
Jul 9, 2019 3:36:29 PM (5min 47s ago)	10.201.0.16	209.182.184.2	spyglass.lancope.com	8616	56453/UDP	219.146.0.253	53/UDP	

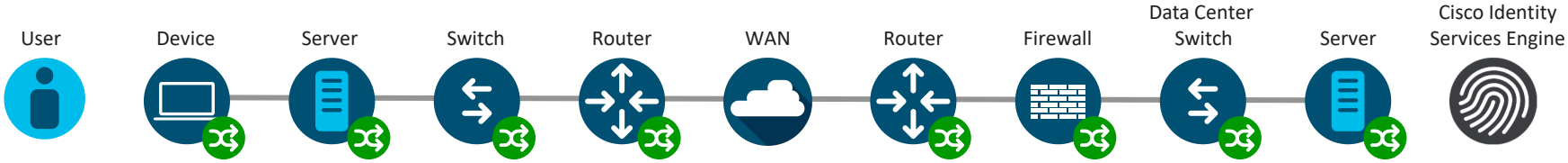
Enriched with data from other sources

Router	Switch	Firewall	Data Center
ISR ASR CSR WLC	Catalyst IE ETA enabled Catalyst	ASA FTD Meraki	Nexus switch Tetration

Web	Endpoint	Policy and User Info	Other
Web Security Appliance (WSA)	AnyConnect	Identity Services Engine (ISE)	Stealthwatch Flow Sensor

Secure Network Analytics also enables telemetry ingestion from many third-party exporters

End-to-End Visibility Infrastructure



NetFlow/sFlow Export is available across the Cisco portfolio

Switch
Catalyst 2960-X (v9/IPFIX)
Catalyst 3650/3850 (v9/IPFIX)
Catalyst 4500E (v9/IPFIX)
Catalyst 6500E (v9/IPFIX)
Catalyst 6800 (v9/IPFIX)
Catalyst 9200 (v9/IPFIX)
Catalyst 9300/9400 (v9/IPFIX ETA)
Catalyst 9500 (v9/IPFIX)
Catalyst 9600 (v9/IPFIX)
IE3000 (v9/IPFIX)
IE4000 (v9/IPFIX)
IE5000 (v9/IPFIX)

Router
Cisco ISR 4000 (v9/IPFIX ETA)
Cisco CSR 1000v (v9/IPFIX ETA)
Cisco ASR 1000 (v9/IPFIX ETA)
Cisco ASR 9000 (v9/IPFIX)
Cisco WLC 5520, 8510, 8540 (v9 Fixed)
Catalyst 9800 (v9/IPFIX ETA)

Firewall
ASA 5500-X (NSEL)
FTD (NSEL)
Meraki MX/Z1 (v9 Fixed)

Data Center Switch
Nexus 1000v (v9/IPFIX)
Nexus 3000 (sFlow)
Nexus 7000 (M Series I/O modules – (v9/IPFIX)
Nexus 7000 (F Series I/O modules – (v9/IPFIX sampled)
Nexus 9000 Series (sFlow)
Nexus 9000 Series EX/FX (v9)

Servers, Software and Appliances
Cisco Stealthwatch Flow Sensor (v9/IPFIX ETA)
Cisco UCS VIC (v9/IPFIX)
Cisco AnyConnect Client (IPFIX)

The above is a non-exhaustive list of Cisco exporters.
For individual platform features, reference the Cisco Feature Navigator: http://cfn.cloudapps.cisco.com/ITDIT/CFN/jsp/index.jsp

Advanced Threat Detection & Response

Monitor hosts and **pinpoint** anomalies using advanced **behavioral modeling**

Detect evolving malware using the power of **multilayered machine learning**

Light up the dark spots by exposing threats hiding in **encrypted traffic**

Advanced detection using behavioral modeling

Comprehensive Data Set

Optimized to remove redundancies and improve performance

Security Events

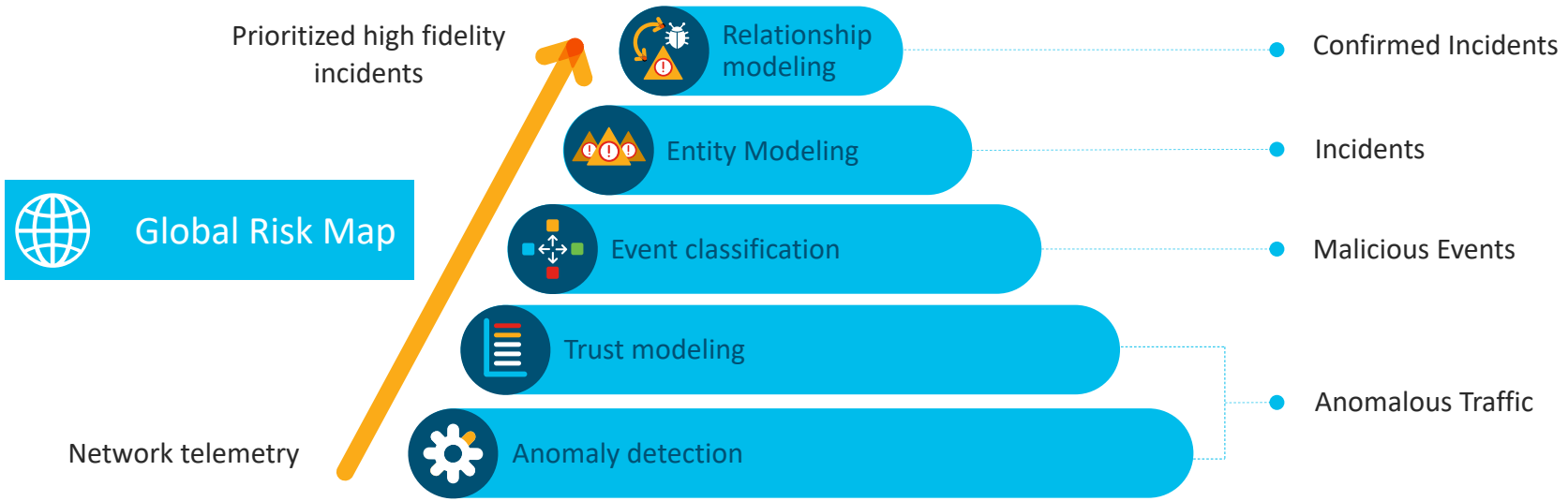
Heuristics to detect anomalies and known bad behavior

Alarm Categories

High-risk, low-noise alerts for faster response

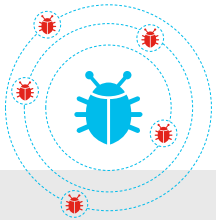
Power of multilayered machine learning

Increase fidelity of detection using best-in-class security analytics

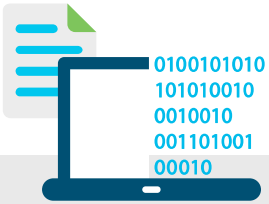


Encrypted Traffic Analytics

Cisco Secure Network Analytics is the only solution providing visibility and malware detection without decryption



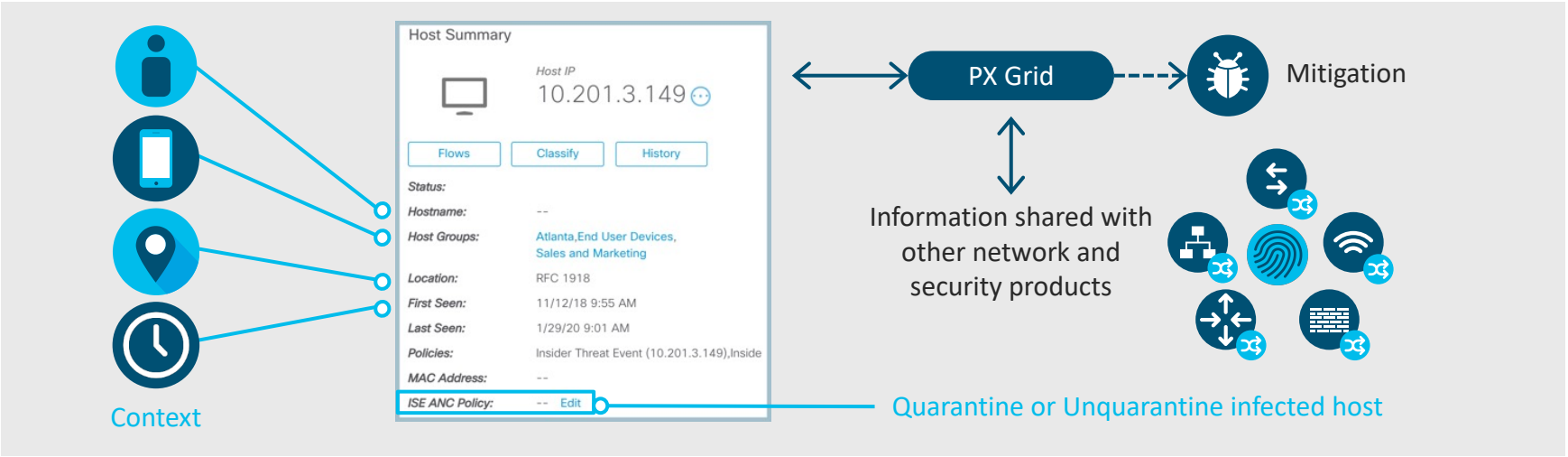
Detect malware in encrypted traffic



Ensure cryptographic compliance

Rapid Threat Containment

Without any business disruption



Cisco®
Identity Services Engine

Stealthwatch
Management Console

Simplified Network Segmentation

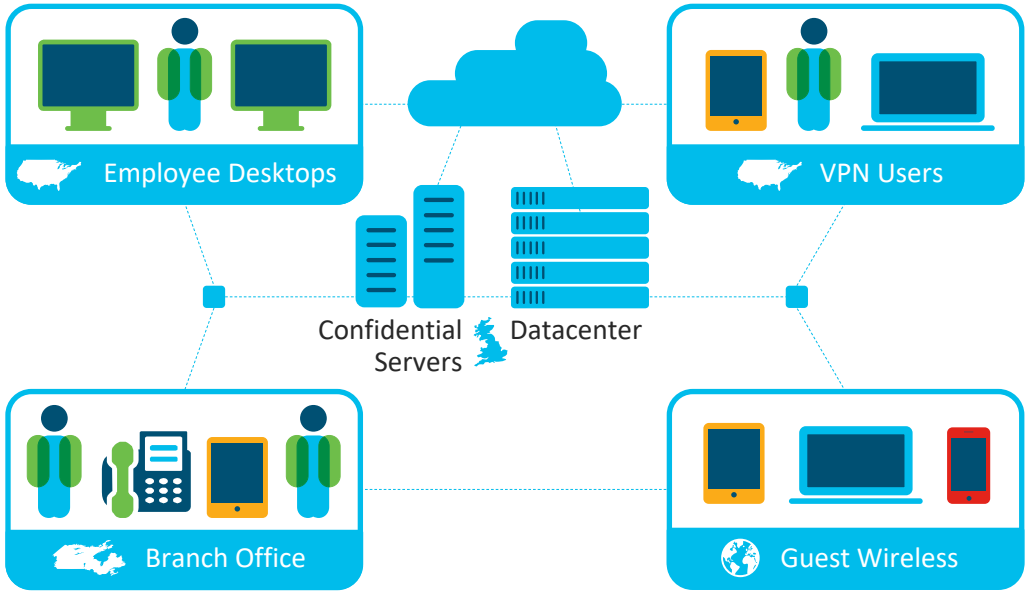
Implement smarter segmentation through complete visibility and behavioral modeling

Create logical groups based on the specific needs of your digital business

Know instantly when **policies are violated**, through contextual alarms

Logical groupings customized to your business

- **Identify** every asset on the network
- **Set policies** based on hosts as well as applications
- **Model policies** before enforcing them



Policy Modeling and Monitoring

“Custom Events” can be created to model policies before enforcing them

Bypass of implemented firewall ACLs

Communication between PoS terminals and the Internet

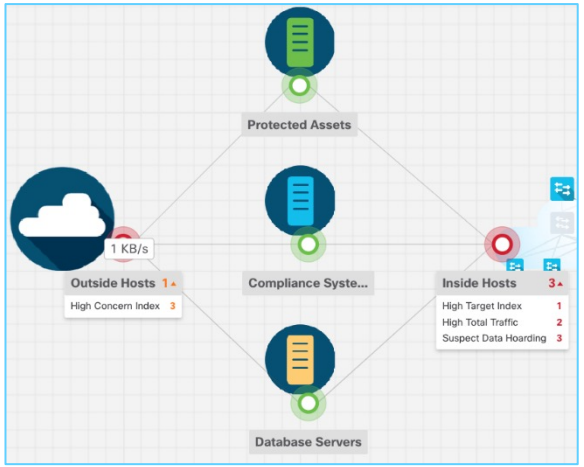
Unapproved communication to servers containing critical or confidential information (PCI, source code data, HR records)

Violation of established communication policy (e.g. no intra-branch location communication)

SMB traffic from inside hosts to outside hosts

Build Maps to Focus on Critical Metrics

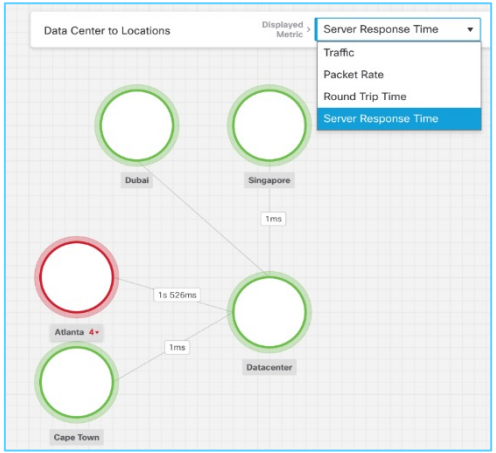
Triggered Alarms



View triggered alarms brief per host groups

Drill down into alarms triggered per host group

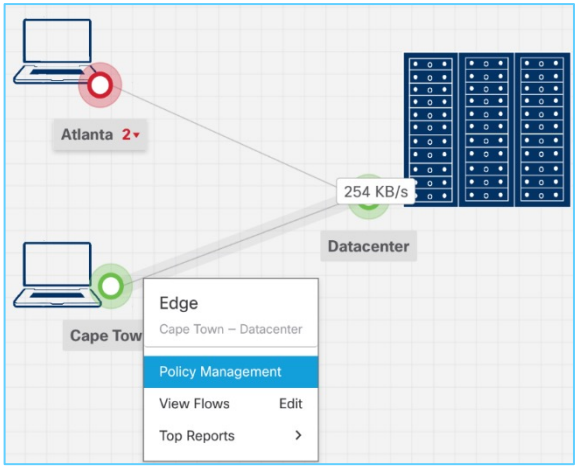
Network Performance



Visualize Network Performance metrics

RTT, SRT, Packet Rate and Traffic bandwidth

Relationship policy



Relationship Policy creation based on graphical representation

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 Secure Network Analytics
- 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 / IPFIX Collector (sFlow FC as well)
- Maximum 25 per deployment

Flow collection license

- Collection, management, and analysis of NetFlow by the Secure Network Analytics system is licensed on the basis of flows per second (FPS) and term.

Management Console

Flow Collector

Flow Collector license

Secure Cloud Analytics

Bringing visibility to what is cloudy

Most companies are using the cloud

evaluating or using public cloud

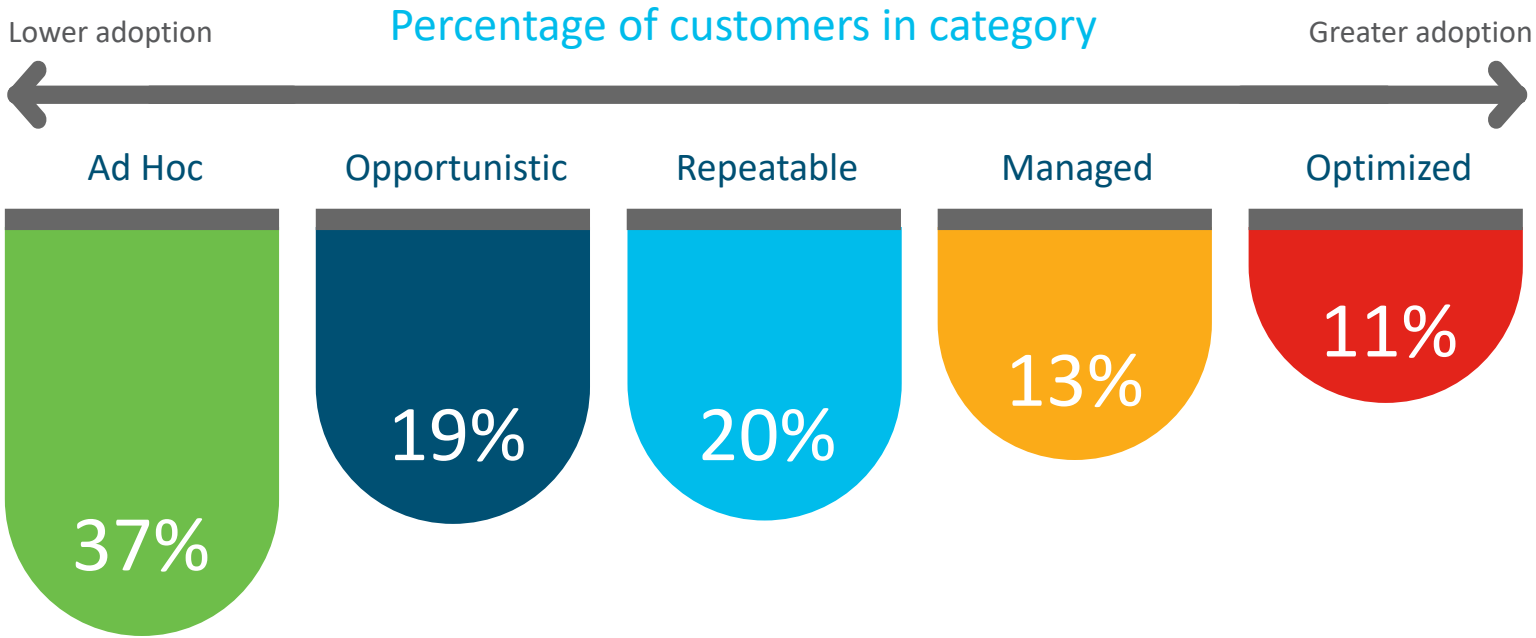
taken steps towards a hybrid cloud strategy

plan to use multiple clouds

Among cloud users

Source: IDC CloudView, April, 2017, n=8,293 worldwide respondents, weighted by country, company size and industry

Cloud Adoption — Only 11% Optimized



IDC CloudView, April, 2018, n=6084 worldwide respondents, weighted by country, company size and industry

Visibility

Achieved by reading flow logs (i.e., NetFlow) directly from the cloud provider

Build an understanding of the network by identifying entity roles based on the traffic

Many cloud workloads are ephemeral, important to know network conversations, even if the resource is no longer active

Threat Detection

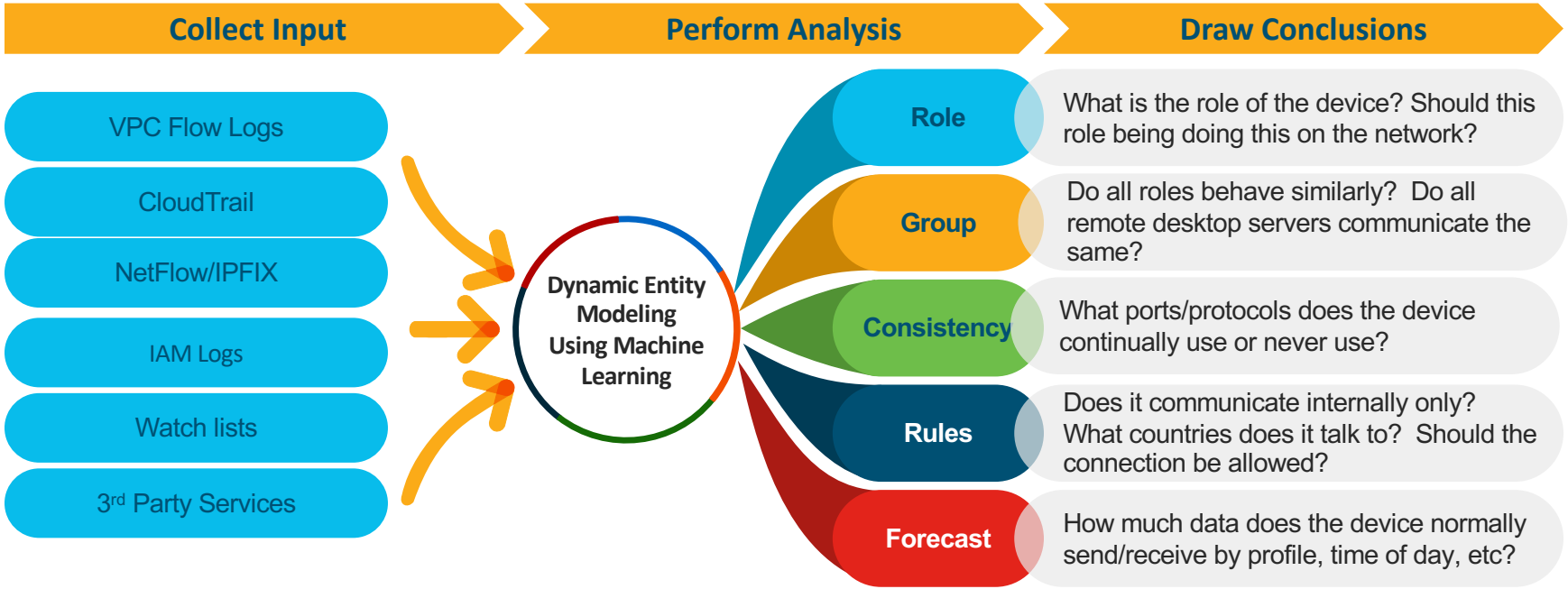
70+ Detections built into the service
30+ active on day 0

Establish baseline, understand normal behavior and identify anomalies over time with ***entity modeling***

Enable smarter response and reduce investigation times with high-fidelity alerts

Machine Learning provides better threat detection

36 Day Baseline



Policy & Compliance

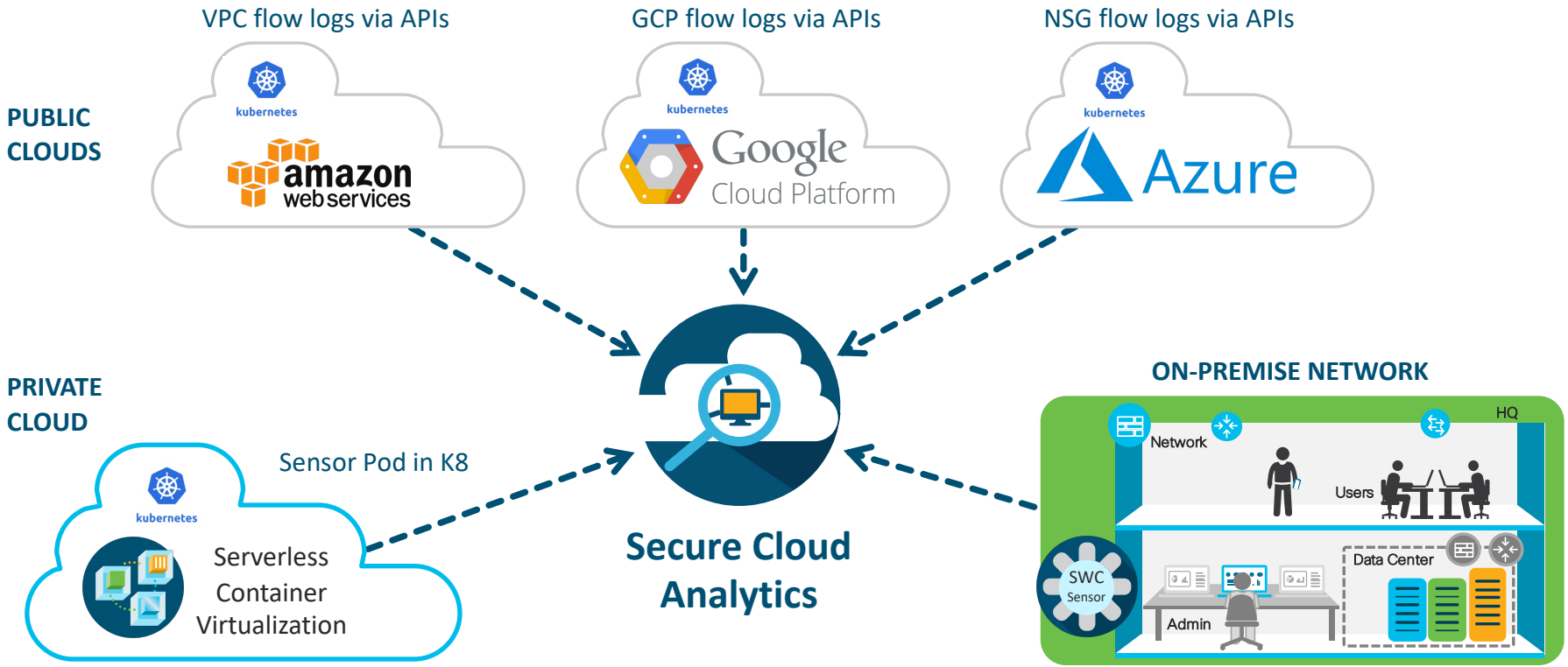
Build custom segmentation rules to check for out of compliance traffic

Talos + Cognitive built-in with options for custom 3rd party watchlists and threat intelligence feeds

Included API for building custom alerts and exporting data to SIEM platforms

cisco Secure

Secure Cloud Analytics - Premises and Public Clouds



Secure Network Analytics Architecture

Comprehensive visibility and security analytics

NetFlow enabled routers, switches, firewalls

Management Console

ISE

Threat Intelligence License

Global Threat Analytics

Secure Cloud Analytics

Other Traffic Analysis Software

Flow Collector

UDP Director

Flow Sensor

VM

VM

Hypervisor with Flow Sensor VE

Telemetry for Encrypted Traffic Analytics

NetFlow enabled routers, switches, firewalls

AnyConnect NVM

Proxy Data

Non-NetFlow enabled equipment


cisco
Secure