Cisco Secure

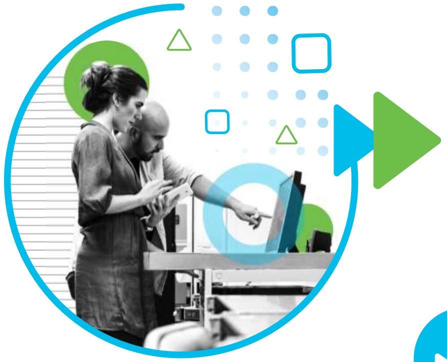
Cisco Security Analytics

Cisco Knowledge Network session

David Butler
Technical Solution Architect

Pramod Nair
Technical Solution Architect

19th Nov 2020

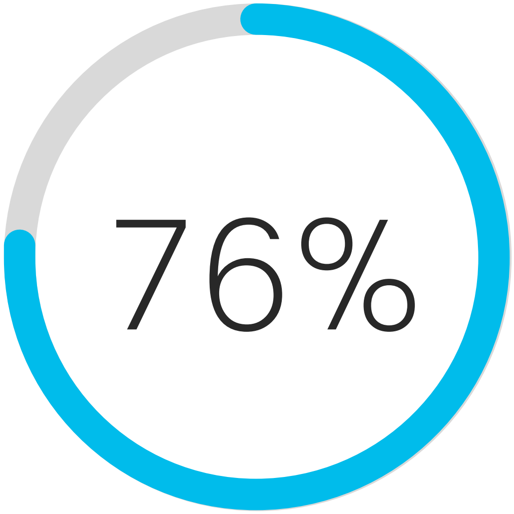


Topics for discussion today

Agenda

- ✓ Cisco Security Analytics overview
- ✓ Secure Analytics use cases for Service Providers

Cisco Secure



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

– The Ponemon Institute

Security Analytics versus Other Analytics

Outcomes

Synthesis/
Analytics

Telemetry

Security Analytics focus on augmenting or automating these functions:

□Incident Responder

□Security Analyst

□Security Operations

□Threat Hunter

□Compliance and Policy

□Business Continuity

□Cybercrime fighting

Could you infer someone's friends by analyzing their phone records?

Infrastructure as a Sensor

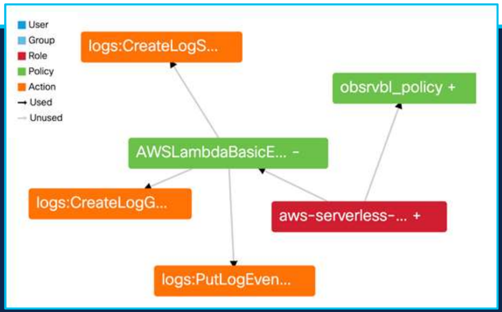
build the general ledger

Native Cloud Telemetry

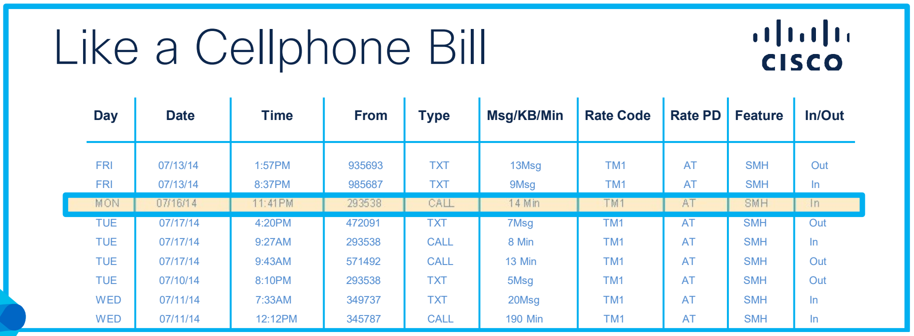
Azure

aws

Google Cloud



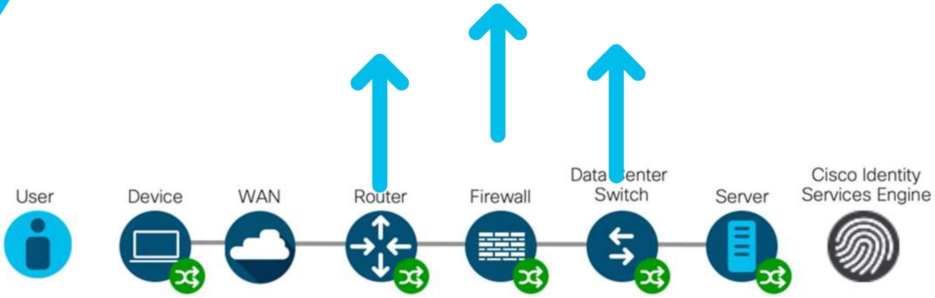
cisco Secure

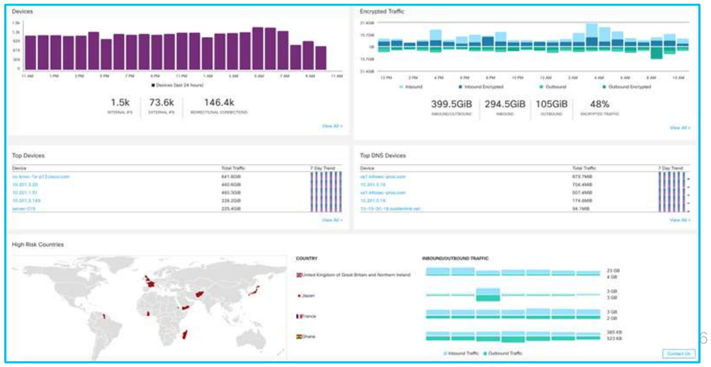


Like a Cellphone Bill

cisco

Day	Date	Time	From	Type	Msg/KB/Min	Rate Code	Rate PD	Feature	In/Out
FRI	07/13/14	1:57PM	935693	TXT	13Msg	TM1	AT	SMH	Out
FRI	07/13/14	8:37PM	985687	TXT	9Msg	TM1	AT	SMH	In
MON	07/16/14	11:41PM	293538	CALL	14 Min	TM1	AT	SMH	In
TUE	07/17/14	4:20PM	472091	TXT	7Msg	TM1	AT	SMH	Out
TUE	07/17/14	9:27AM	293538	CALL	8 Min	TM1	AT	SMH	In
TUE	07/17/14	9:43AM	571492	CALL	13 Min	TM1	AT	SMH	Out
TUE	07/10/14	8:10PM	293538	TXT	5Msg	TM1	AT	SMH	Out
WED	07/11/14	7:33AM	349737	TXT	20Msg	TM1	AT	SMH	In
WED	07/11/14	12:12PM	345787	CALL	190 Min	TM1	AT	SMH	In





Effective Security Depends on Total Visibility

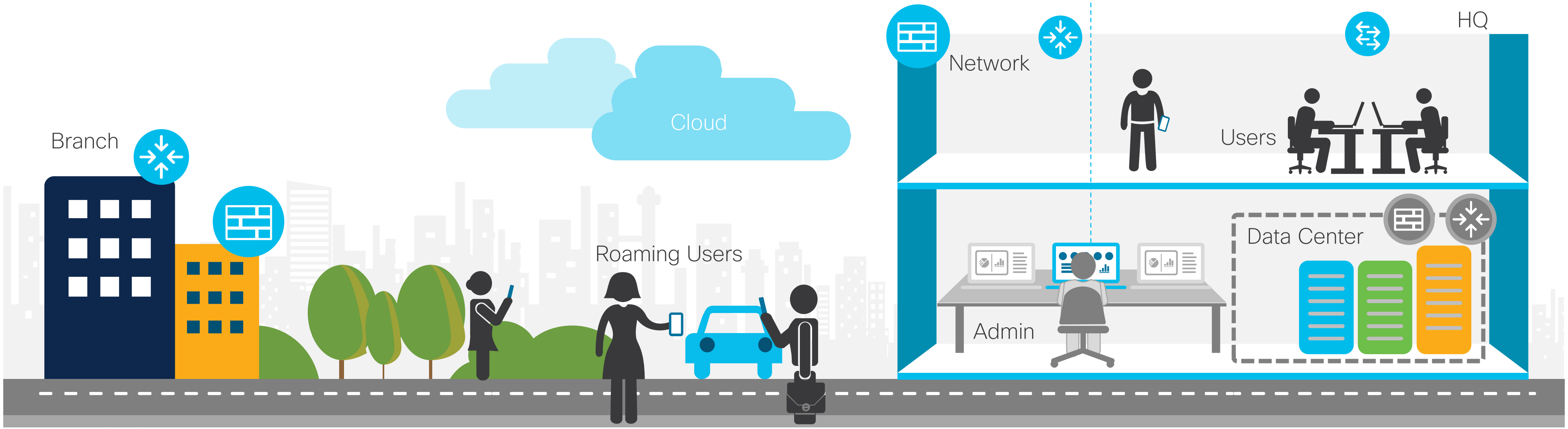
KNOW
every host

SEE
every conversation

Understand what
is NORMAL

Be alerted to
CHANGE

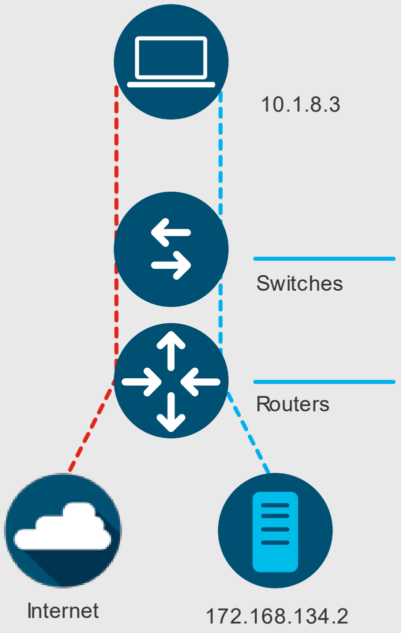
Respond to
THREATS quickly



The infrastructure as a sensor

See it ALL!

- A Trace of every conversation
- Agentless information collection
- East West and North South visibility
- Light Meta Data Collection using the existing infrastructure



Flow Information	Packets
SOURCE ADDRESS	10.1.8.3
DESTINATION ADDRESS	172.168.134.2
SOURCE PORT	47321
DESTINATION PORT	443
INTERFACE	Gi0/0/1
IP TOS	0x00
IP PROTOCOL	6
NEXT HOP	172.168.25.1
TCP FLAGS	0x1A
SOURCE SGT	100
:	:
ETA Meta Data	IDP | SPLT
APPLICATION NAME	NBAR SECURE- HTTP

cisco Secure

The magic of machine learning

ML uses models to tackle new issues in real time without human intervention

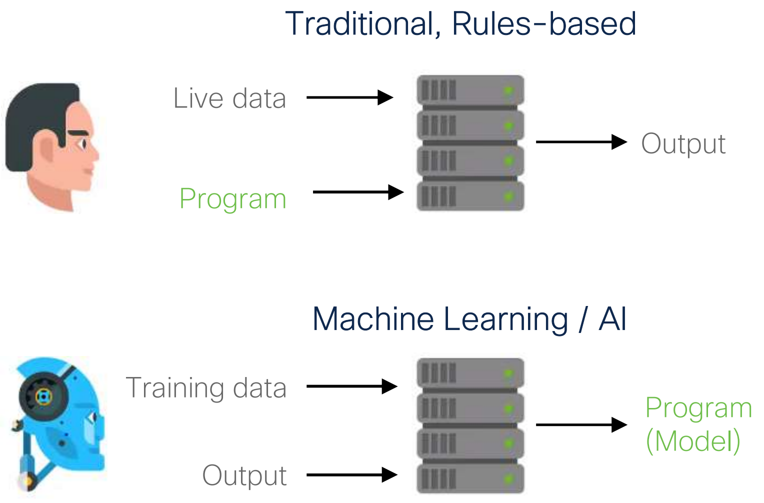
Machine Learning Definitions

Arthur Samuel (1959)

Field of study that gives computers the ability to learn without being explicitly programmed

Tom Mitchell (1997)

A computer program is said to learn if its performance at a task T, as measured by a performance P, improves with experience E



Traditional, Rules-based

Live data → Output

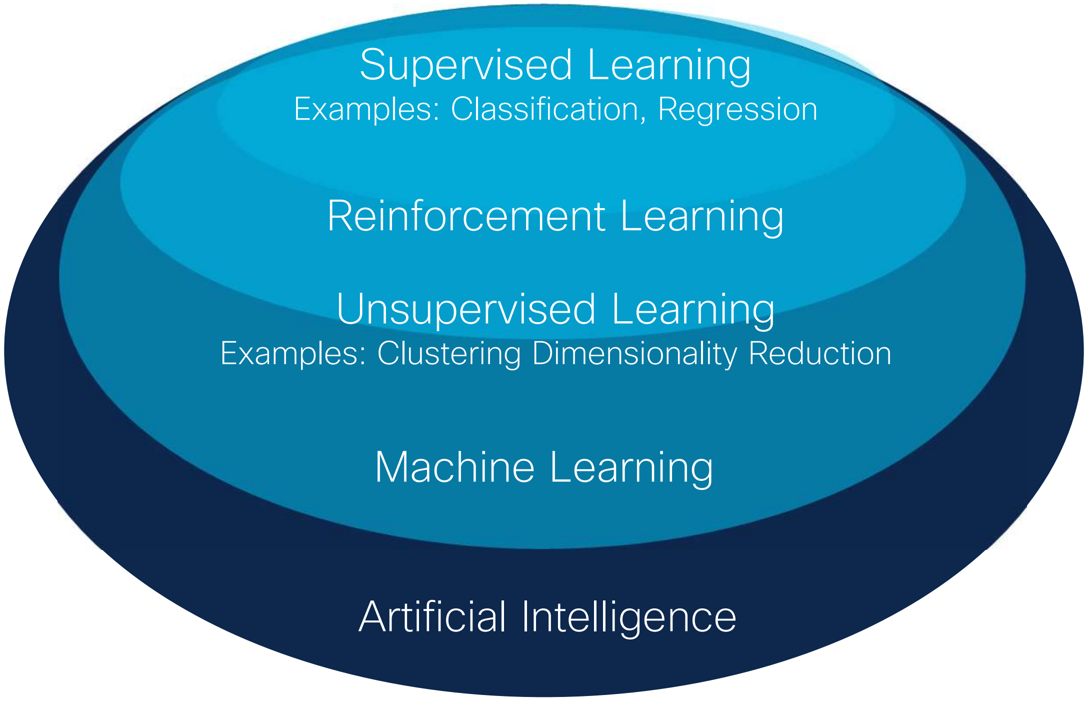
Program →

Machine Learning / AI

Training data → Program (Model)

Output →

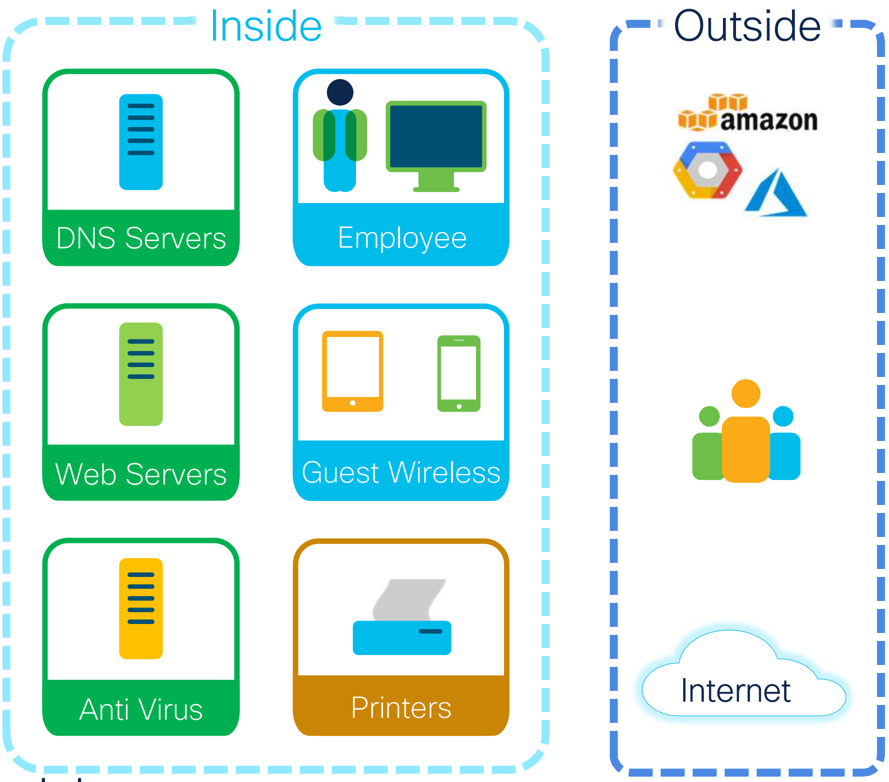
Machine Learning Big Picture



Machine Learning is ***one*** of the fields in Artificial Intelligence, where machines learn to act autonomously, and react to new situations ***without being pre-programmed***. It is about designing algorithms that allow computers to learn aimed at some outcome.

- Learn to identify faces, learn to drive a car, etc
- Learning to detect malware, learning to identify a threat actors, etc.

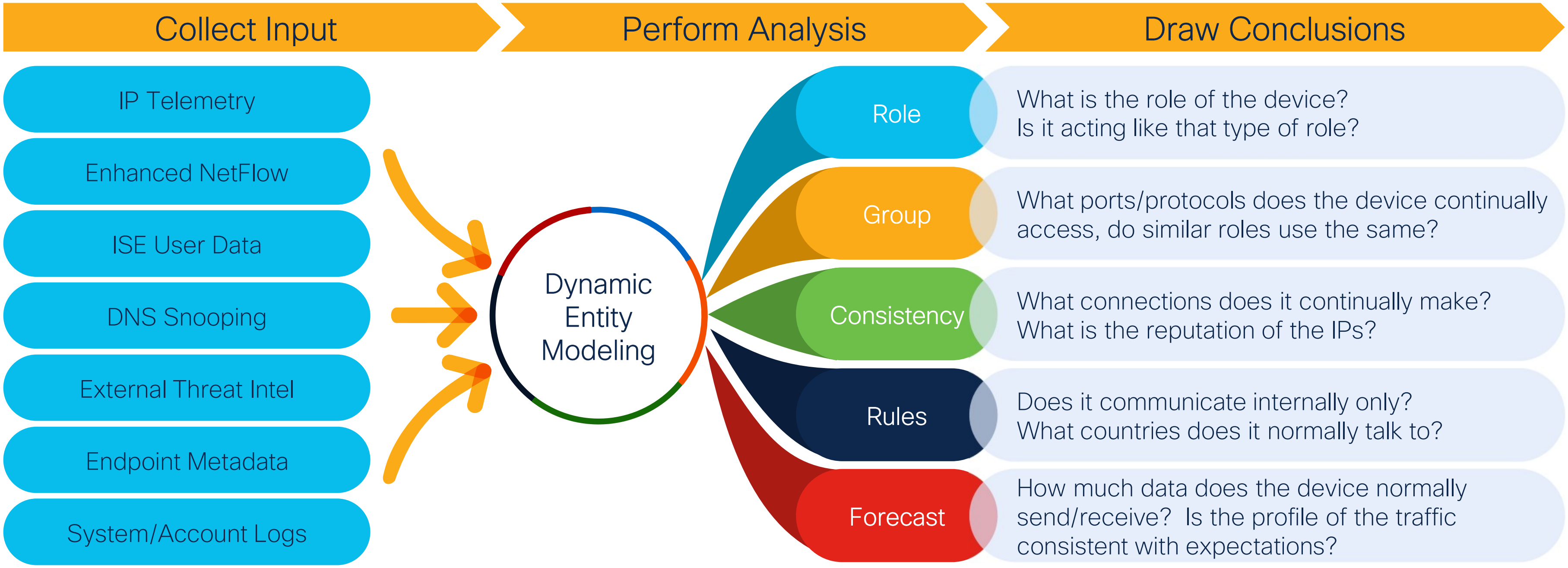
Functional Network Segmentation by Groups



- A host group is grouping of hosts that share attributes and policies
- Host group are monitored to establish baseline behavior and thresholds
- Alerts are sent when hosts behave outside the group behavior
- 4 Ways to Segment
  1. Manual Host Group Creation
  2. APIs using IPAM, IND, Threat Intelligence data
  3. Host Classifier App
  4. Host Group Automation Service

cisco Secure

Entity Modeling to Baseline and Detect Behavior Changes



Collect Input

- IP Telemetry
- Enhanced NetFlow
- ISE User Data
- DNS Snooping
- External Threat Intel
- Endpoint Metadata
- System/Account Logs

Perform Analysis

Dynamic Entity Modeling

Draw Conclusions

Role: What is the role of the device? Is it acting like that type of role?

Group: What ports/protocols does the device continually access, do similar roles use the same?

Consistency: What connections does it continually make? What is the reputation of the IPs?

Rules: Does it communicate internally only? What countries does it normally talk to?

Forecast: How much data does the device normally send/receive? Is the profile of the traffic consistent with expectations?

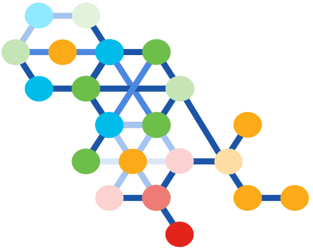
Cognitive Intelligence

Beyond Machine Learning

Anomaly Detection
Behavioral Analytics
Host Categorization

Threat Classification
Threat Actor Models
Global Risk Map

Billons of network flows per day
Millions of protected devices
1500+ customers



12 Years of research
70 ML scientists and engineers
60+ Patents & filings
200+ Publications

Polymorphic & Emerging Threats

Cross-product correlation for malware detection
Predicting evolving threat infrastructure

Agentless Malware Detection

File-less, memory-only malware
Process and network behavioral analysis

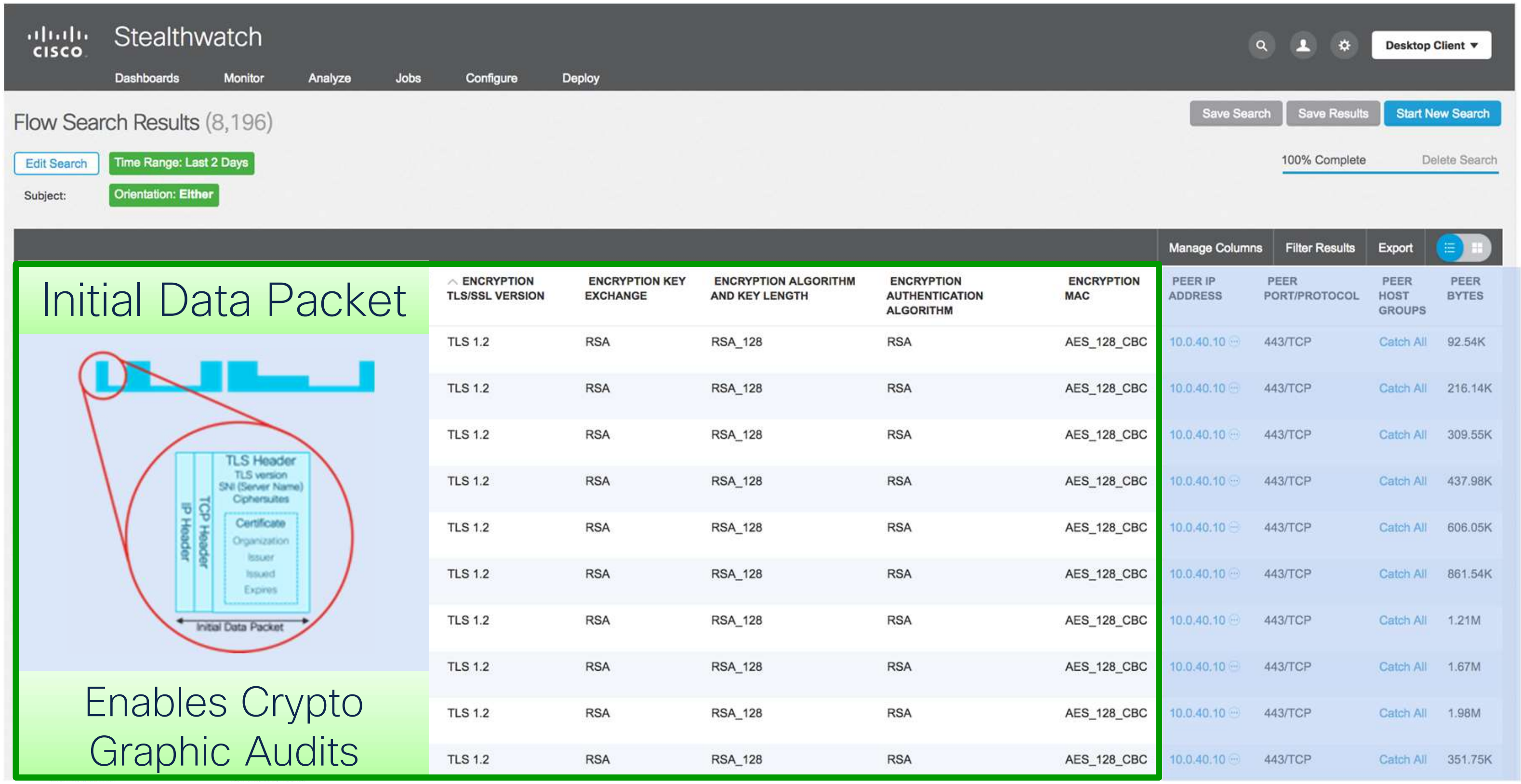
Web Proxy as a Sensor

Behavioral Breach Detection
Detection of infections bypassing the perimeter

Encrypted Traffic Analytics

Netflow & ETA analytics
Behavioral Breach Detection

Cryptographic Visibility

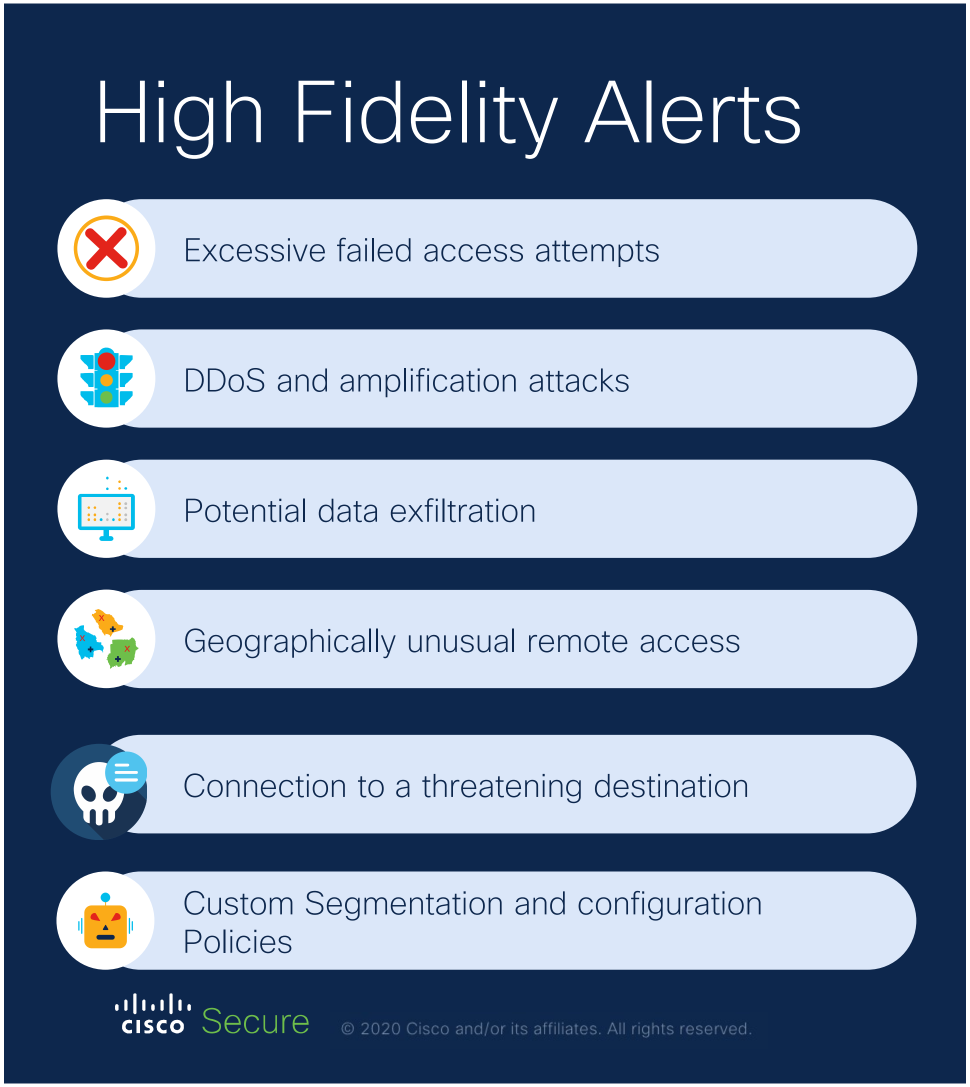


Flow Search Results (8,196)

Initial Data Packet

Enables Crypto Graphic Audits

ENCRYPTION TLS/SSL VERSION	ENCRYPTION KEY EXCHANGE	ENCRYPTION ALGORITHM AND KEY LENGTH	ENCRYPTION AUTHENTICATION ALGORITHM	ENCRYPTION MAC	PEER IP ADDRESS	PEER PORT/PROTOCOL	PEER HOST GROUPS	PEER BYTES
TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	92.54K
TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	216.14K
TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	309.55K
TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	437.98K
TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	606.05K
TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	861.54K
TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.21M
TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.67M
TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.98M
TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	351.75K



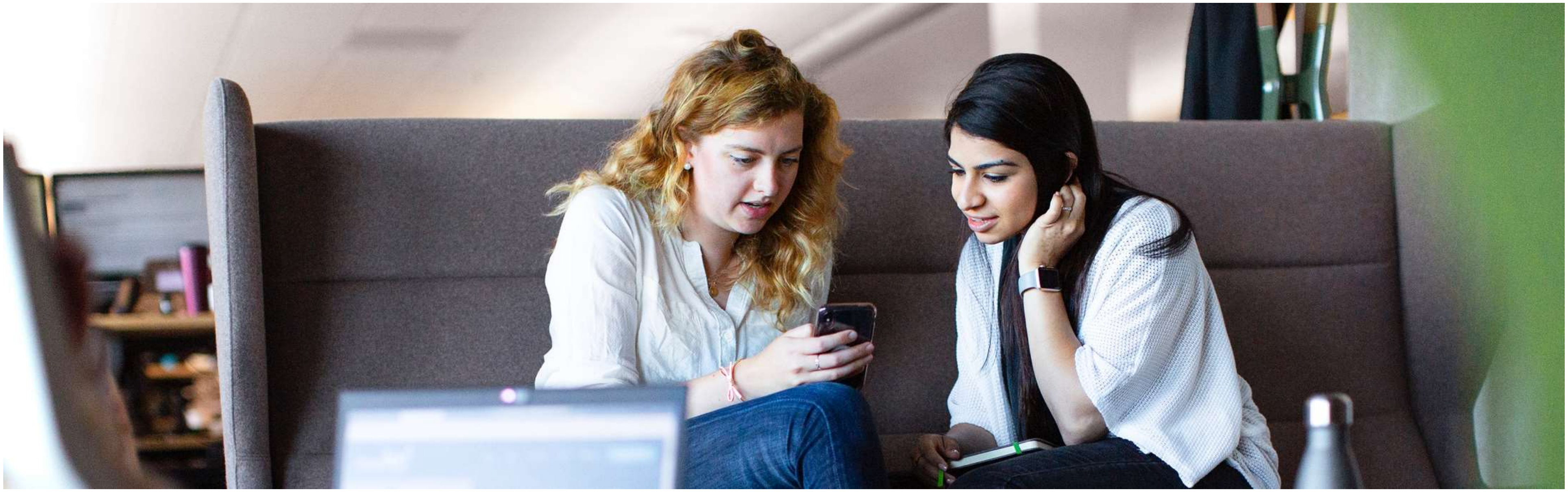
High Fidelity Alerts

- Excessive failed access attempts
- DDoS and amplification attacks
- Potential data exfiltration
- Geographically unusual remote access
- Connection to a threatening destination
- Custom Segmentation and configuration Policies

Automatic Threat Detection

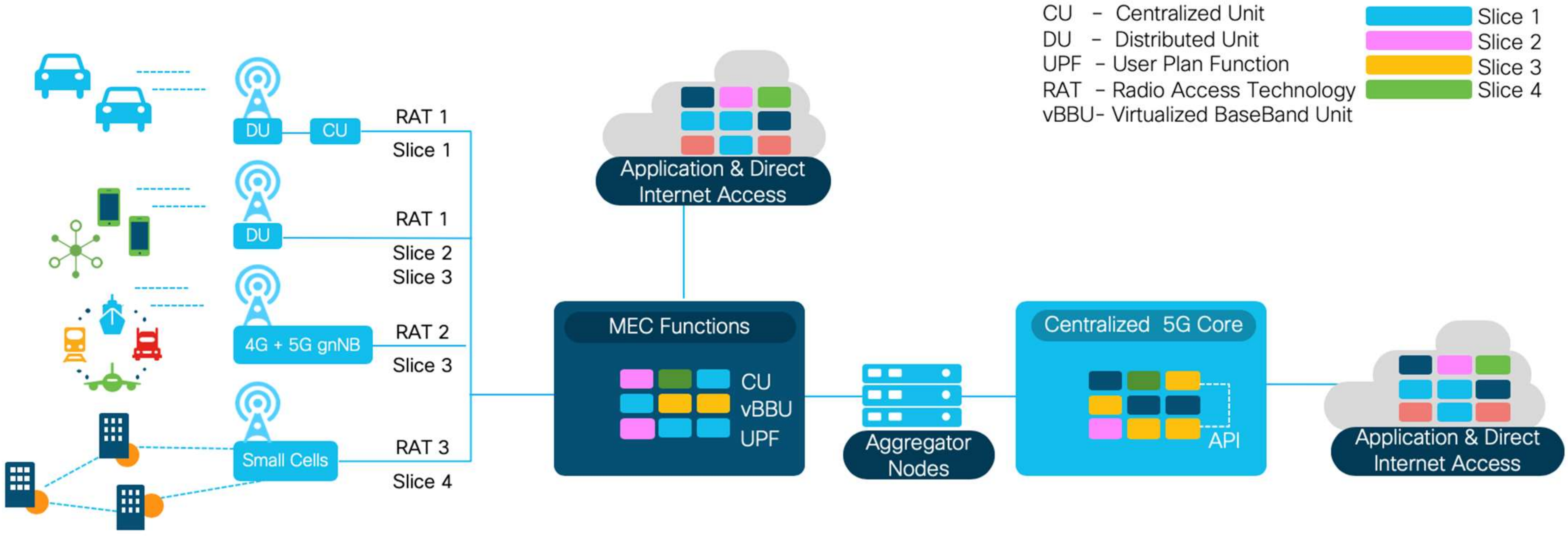
ALERT: Anomaly detected

90% Stealthwatch Cloud alerts rated as “helpful” by customers



Security Analytics Use cases for Service Providers

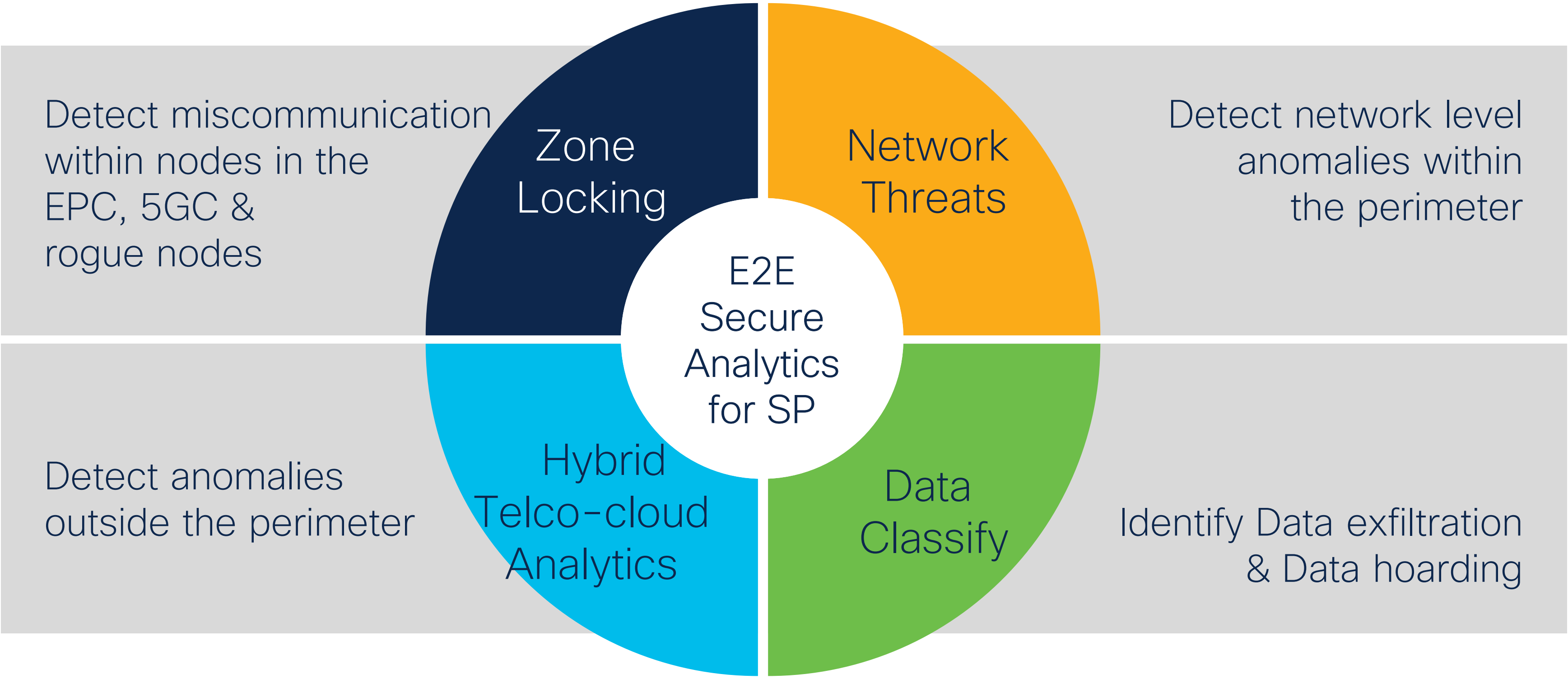
5G & Evolving SP architectures



CU - Centralized Unit
DU - Distributed Unit
UPF - User Plan Function
RAT - Radio Access Technology
vBBU- Virtualized BaseBand Unit

🟦 Slice 1
🟪 Slice 2
🟨 Slice 3
🟩 Slice 4

Use cases for discussion today



E2E Secure Analytics for SP

Zone Locking

Detect miscommunication within nodes in the EPC, 5GC & rogue nodes

Network Threats

Detect network level anomalies within the perimeter

Hybrid Telco-cloud Analytics

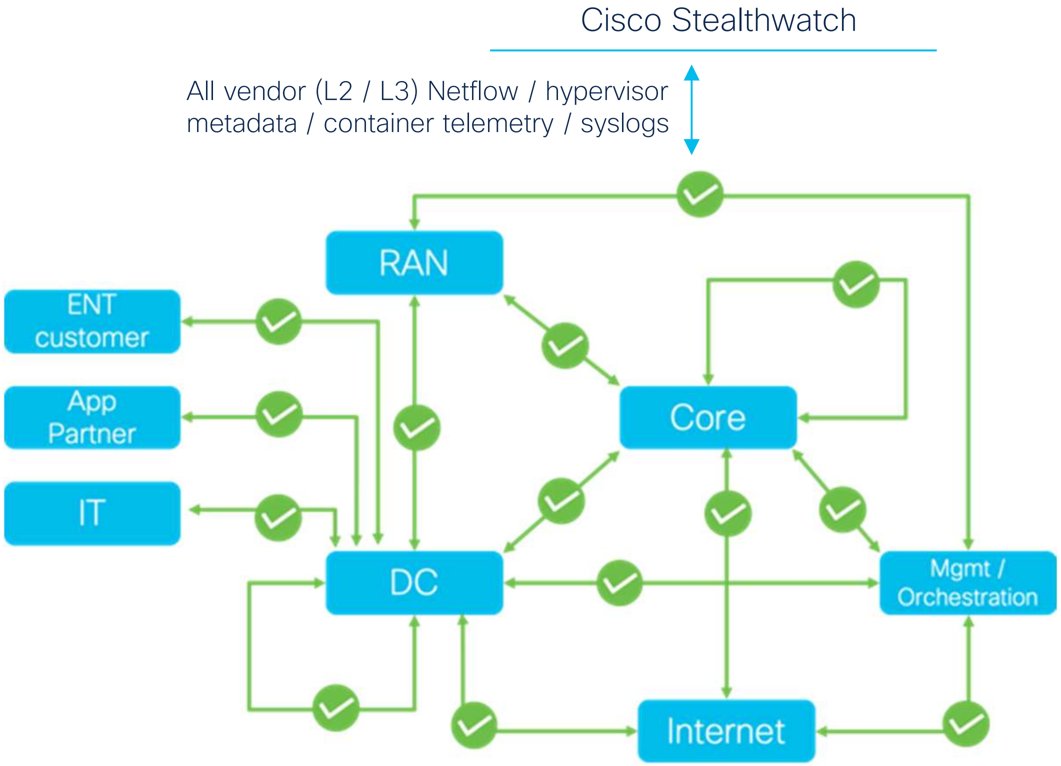
Detect anomalies outside the perimeter

Data Classify

Identify Data exfiltration & Data hoarding

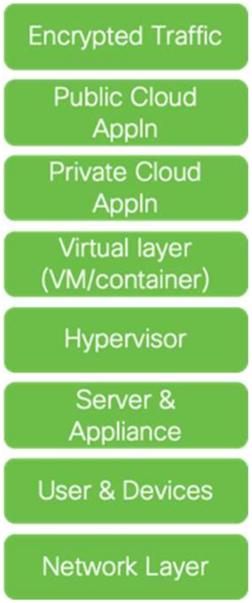
E2E monitoring for multi-vendor 5G networks

(Control Plane, Management & Service layer)


Cisco Stealthwatch
All vendor (L2 / L3) Netflow / hypervisor metadata / container telemetry / syslogs
RAN
ENT customer
App Partner
IT
Core
DC
Mgmt / Orchestration
Internet

End to End monitoring – details

Multi-vendor components



Encrypted Traffic

Public Cloud Appln

Private Cloud Appln

Virtual layer (VM/container)

Hypervisor

Server & Appliance

User & Devices

Network Layer

Gathered network intelligence

NetFlow

IPFIX

VPC logs

sFlow

Container Telemetry

metadata

NSEL

syslogs

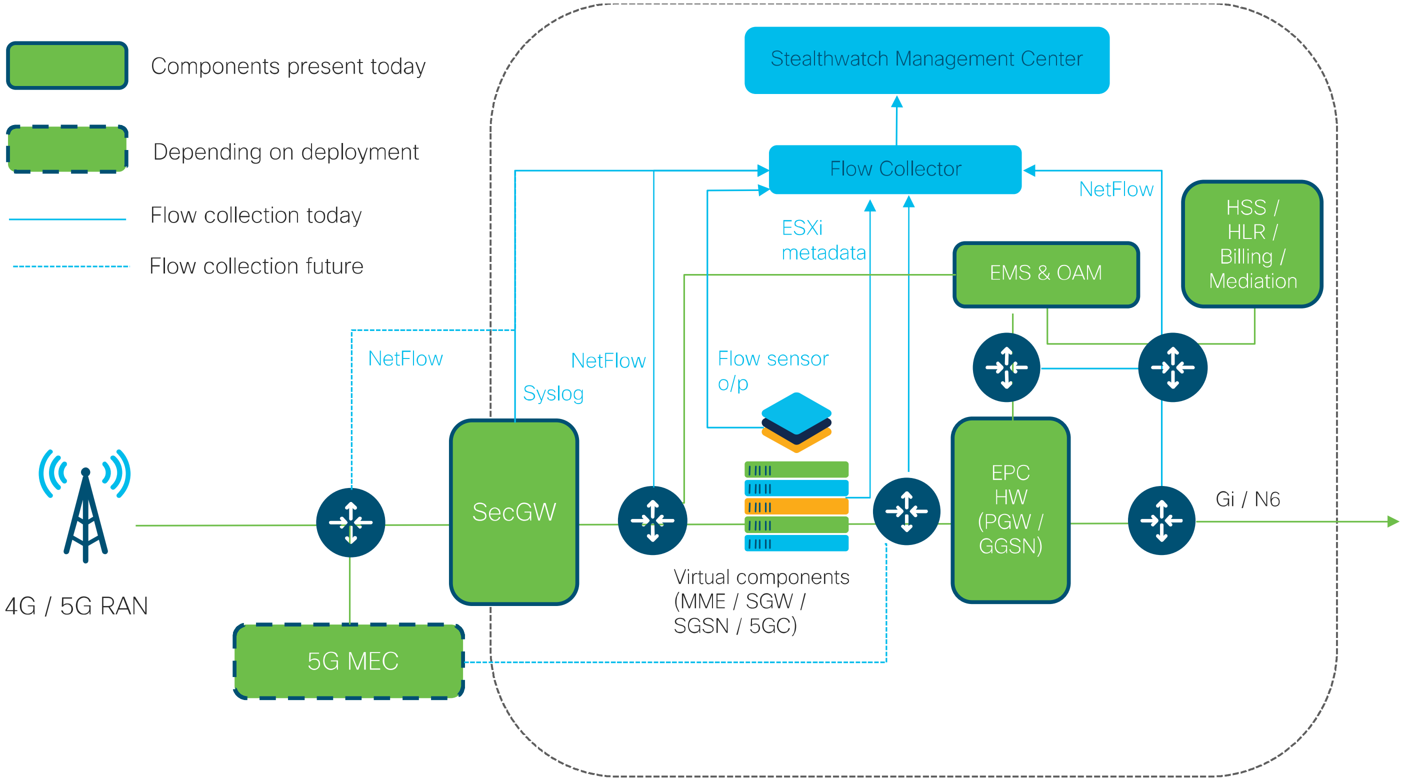
Sample Outcome

- Data exfiltration detection
- Data hoarding detection
- Encryption auditing
- Detect Peer to Peer traffic
- Detecting malware propagation
- Detect network scanning
- Detecting unknown applications
- Verifying change control management

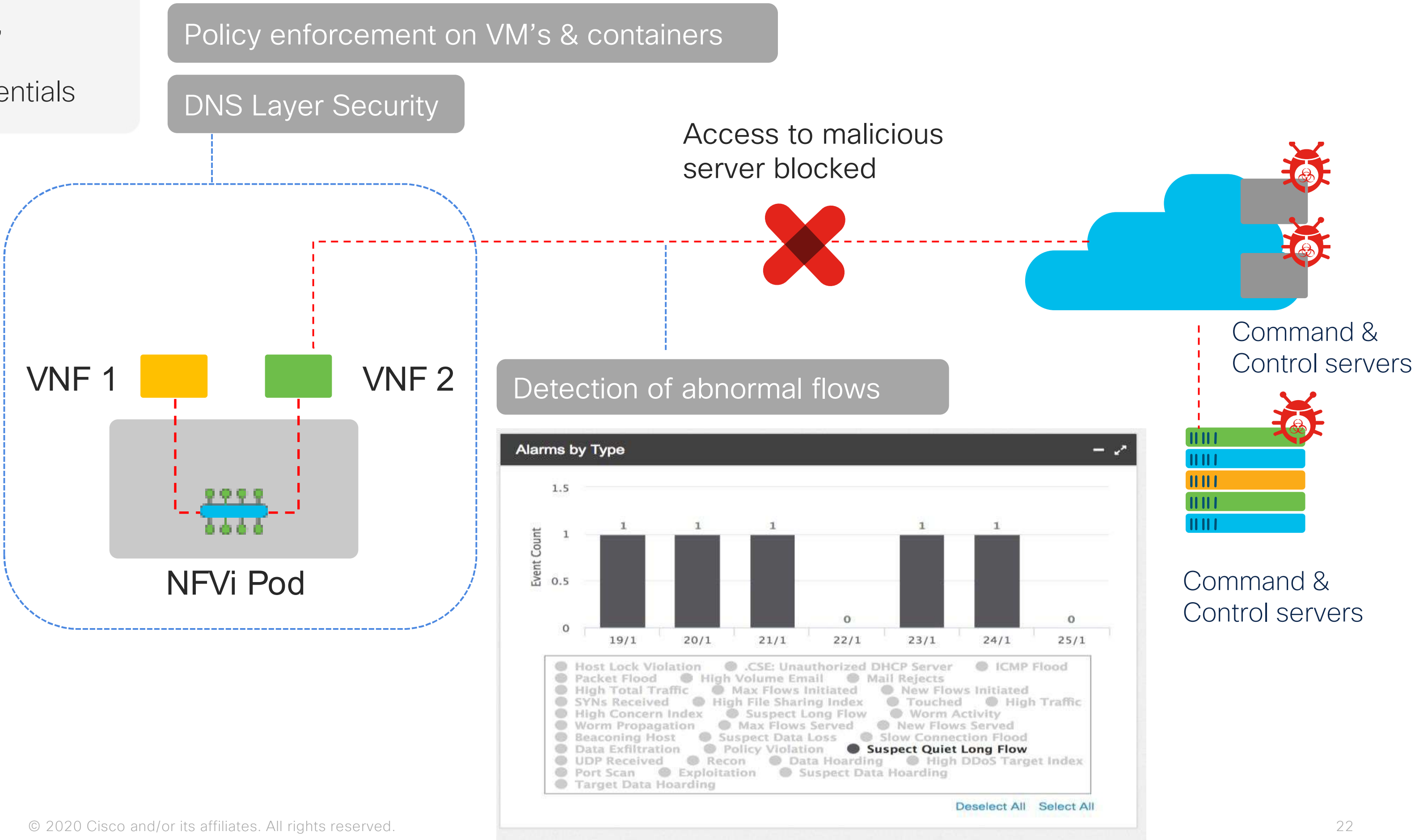
Helping Incident response teams using Stealthwatch monitoring:
https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/white-paper-c11-737531.pdf

Deployment illustration

(Actual customer design)



Problem | Virtualization / Container vulnerabilities (External & Internal), Privilege misuse, Compromised credentials



Policy enforcement on VM’s & containers

DNS Layer Security

Access to malicious server blocked

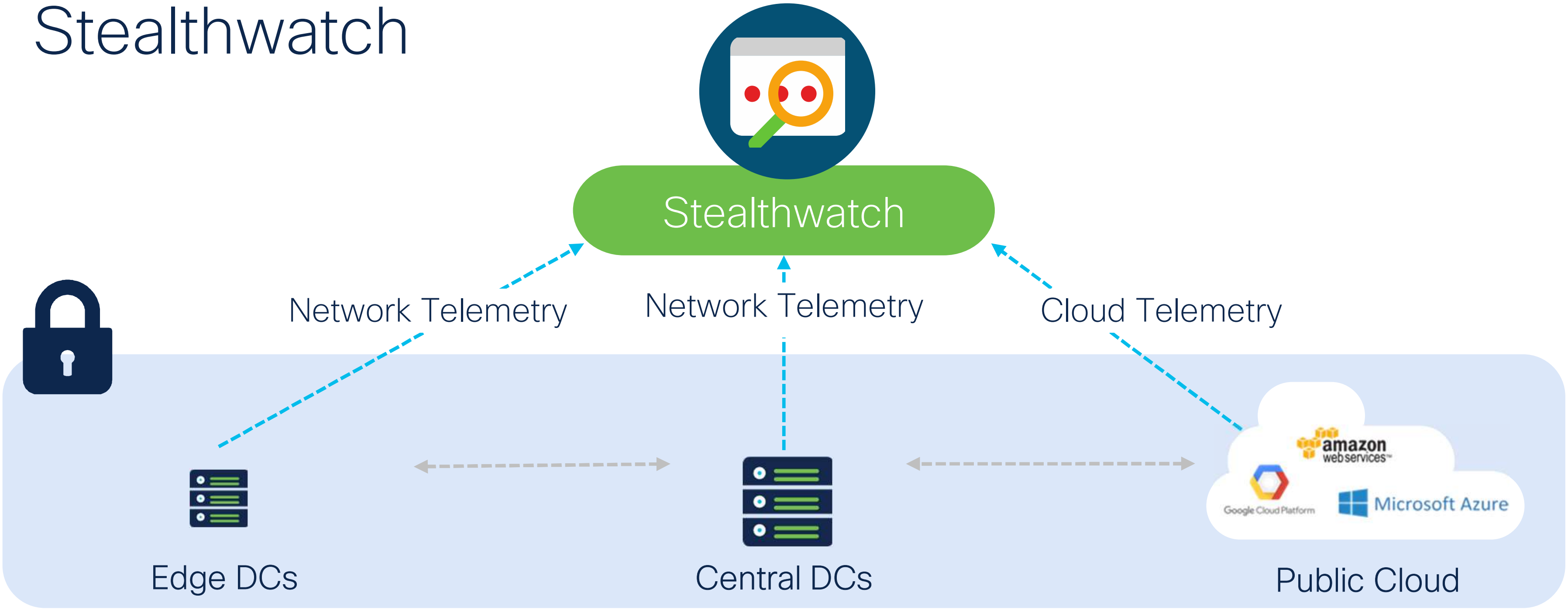
Detection of abnormal flows

Command & Control servers

Command & Control servers

cisco Secure

5G Hybrid cloud Security Analytics using Stealthwatch



Contextual network-wide visibility

Agentless, using existing network and cloud infrastructure, even in encrypted traffic

Predictive threat analytics

Combination of behavioral modeling, machine learning and global threat intelligence

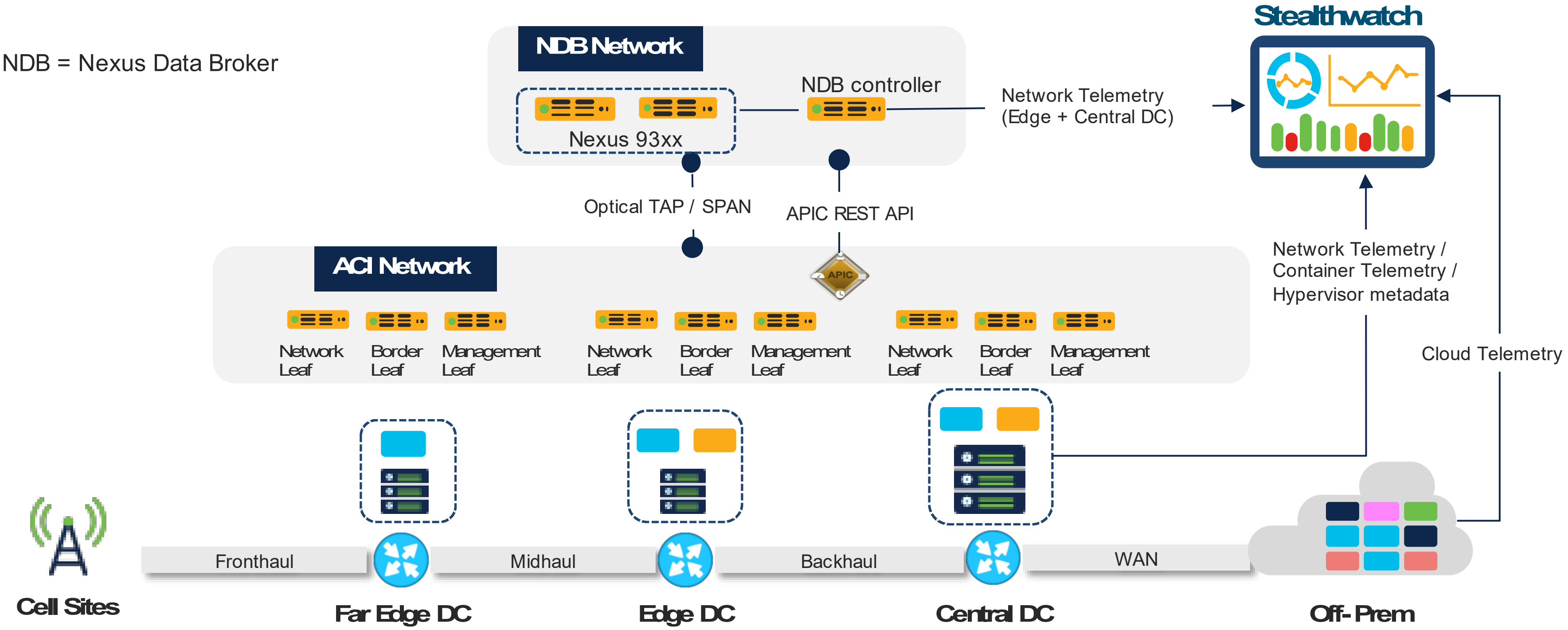
Automated Detection and Response

High-fidelity alerts prioritized by threat severity with ability to conduct forensic analysis

5G Telco cloud Analytics - edge and central DC

(actual design for a customer)

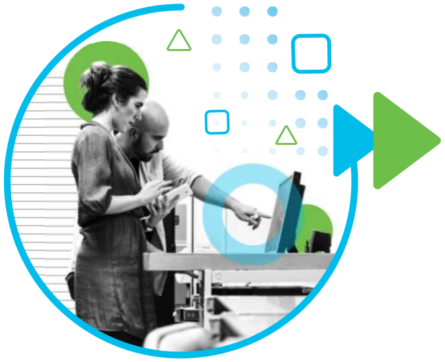
NDB = Nexus Data Broker



Nexus Data Broker:
https://www.cisco.com/c/en/us/products/cloud-systems-management/nexus-data-broker/index.html

Key Takeaways

- Evolving architectures in SP's require enhanced visibility and anomaly detection methods to prevent data exfiltration
- Methods like Encrypted Traffic Analytics (ETA) should be applied at encrypted interfaces to detect malicious traffic without the need for decryption
- 5G E2E monitoring is very important to ensure enhanced security posture, which can be achieved by, monitoring the control plane



Questions?

cisco Secure