Stealthwatch

Network as a Sensor and Enforcer

Network visibility and security intelligence

Marcus Josefsson
Stealthwatch Lead MEAR

Cisco Security Summit - Kiev

Agenda

- Overview and value
- Network as a Sensor
- NW performance monitoring
- Network as an Enforcer
- Architecture & Summary
- Short demo

Cisco StealthWatch

Using Netflow/NSEL/NBAR/Syslog

Without relaying using of probes and agents

Cisco ISE integration

Finish Line

Edward Snowden example

Cisco - Lancope

- **Cisco is Lancope Customer since 2011**

- **Lancope Part of Cisco Security Products since 2013**

- **Cyber Threat Defense (2013)**

  Lancope provides visibility, behavior analysis, incident response and forensic as part of the Cisco Cyber Thread Defense (CTD) solution offered by Cisco

- **NaaS and NaaE (2014)**

  Lancope provide the sensor for the Cisco networking solutions as part of the Network as a Sensor and Network as an Enforcer architecture.
  (Marcus leaves Cisco after 9 years)

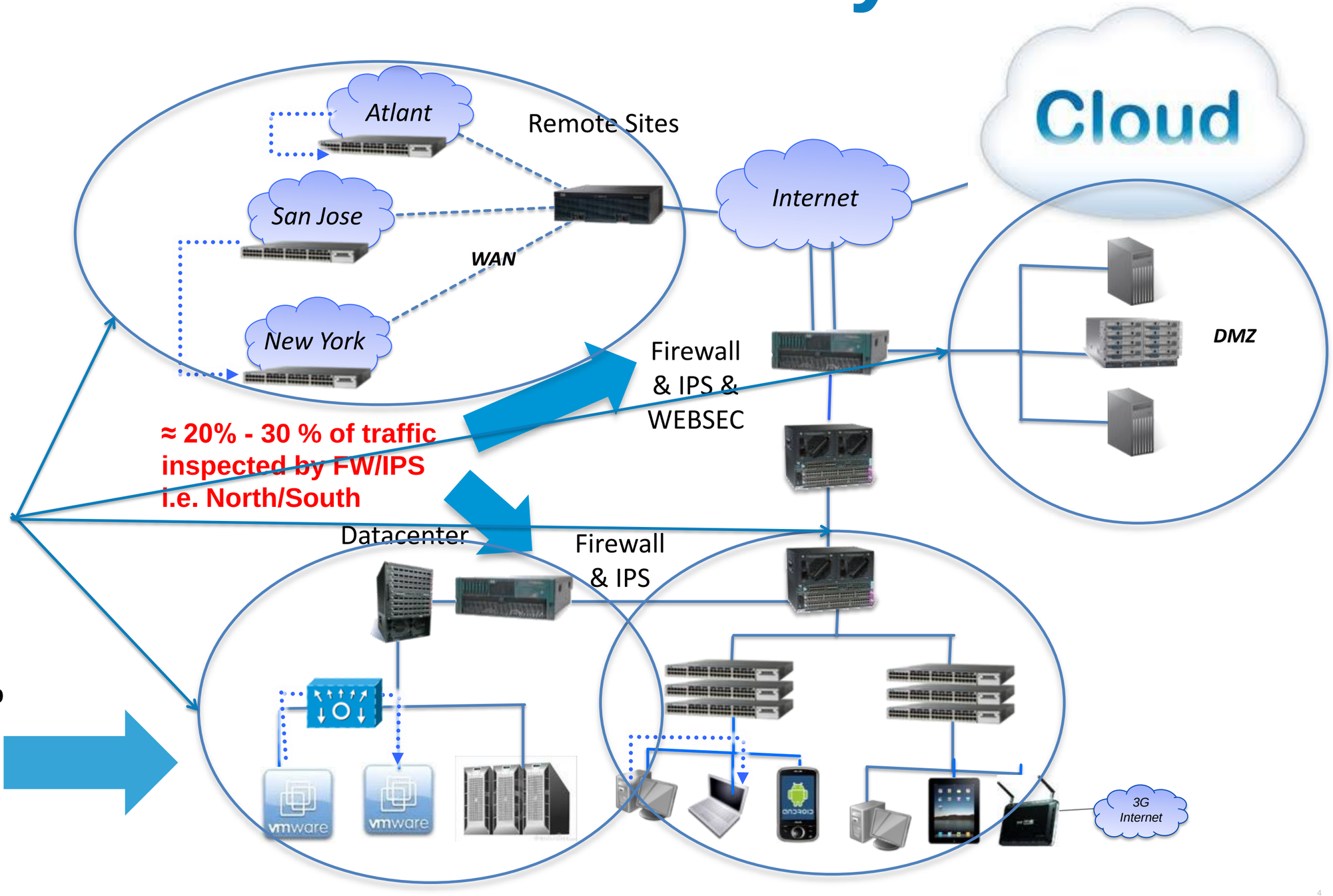
- **Cisco aquires Lancope (Jan 2016)**

  At a cost of 850M USD
  (Marcus back at Cisco 18 months @ Lancope)

Why we need more visibility:

≈ 60% - 90 % of traffic goes unexpected

Typically ≈ 60+ % of total traffic is DC East/West



The value of Stealthwatch

Extended visibility

- Continuously monitor devices, applications and users throughout distributed networks
- Aggregate and analyze advanced telemetry to establish a network security baseline

Policy and access management

- Monitor the entire network and data center to ensure that there are no policy or network access violations

Advanced threat protection

- Obtain contextual threat intelligence with historic audit trail of NetFlow data
- Achieve enhanced visibility and context to accelerate threat detection

Forensics and incident response

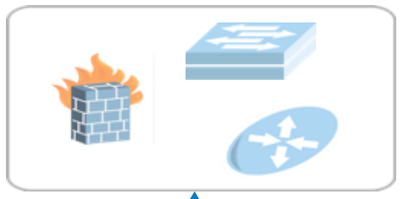
- Improve incident response and forensic analysis through actionable intelligence
- Isolate the root cause of an incident within seconds or months later for mitigation/root cause analysis
- Extensive network performance management feature set

StealthWatch – high level architecture

Forward flow data to StealthWatch for Instant detection, Reporting, Forensics and Enforcement

Switching, Routing,
Data Center, Firewall

Flow Telemetry
Netflow/Ipfix
NSEL an NBAR



Flow

STEALTH WATCH By Lancope

Context

Identity, MAC Address, Device Type,
Reputation, Application, Location,
Posture, NAT, Permit/Deny etc

Network Enforcement/pXGrid

Threat Telemetry/pXGrid

PS engagement or Cisco ISE

Out-of-the-box reporting

SysLog

SMTP

Timeline Security Operations Centre

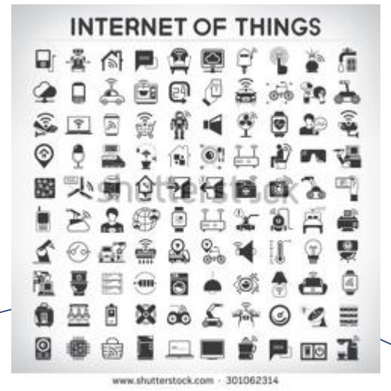
IOC (Indicator of Compromise)

13:06:15:
Internal host
Visits malicious
Web Site

13:07:00:
Gateway malware
analysis identifies the
transaction as malicious

13:14:00:
Administrators Manually
disconnect the infected
host

Use Case – Targeted Attack

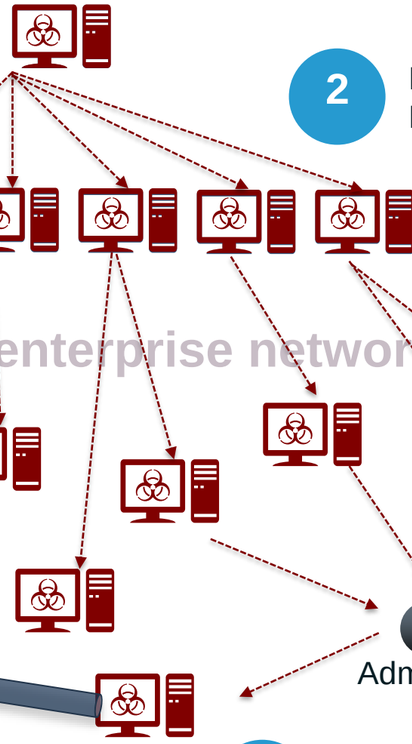


Perimeter
(Inbound)

1 **Infiltration and Backdoor establishment**

Attacker

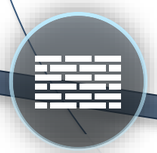
C2 Server



enterprise network

2 **Reconnaissance and Network Traversal**

5 **Data Exfiltration**



Perimeter
(Outbound)

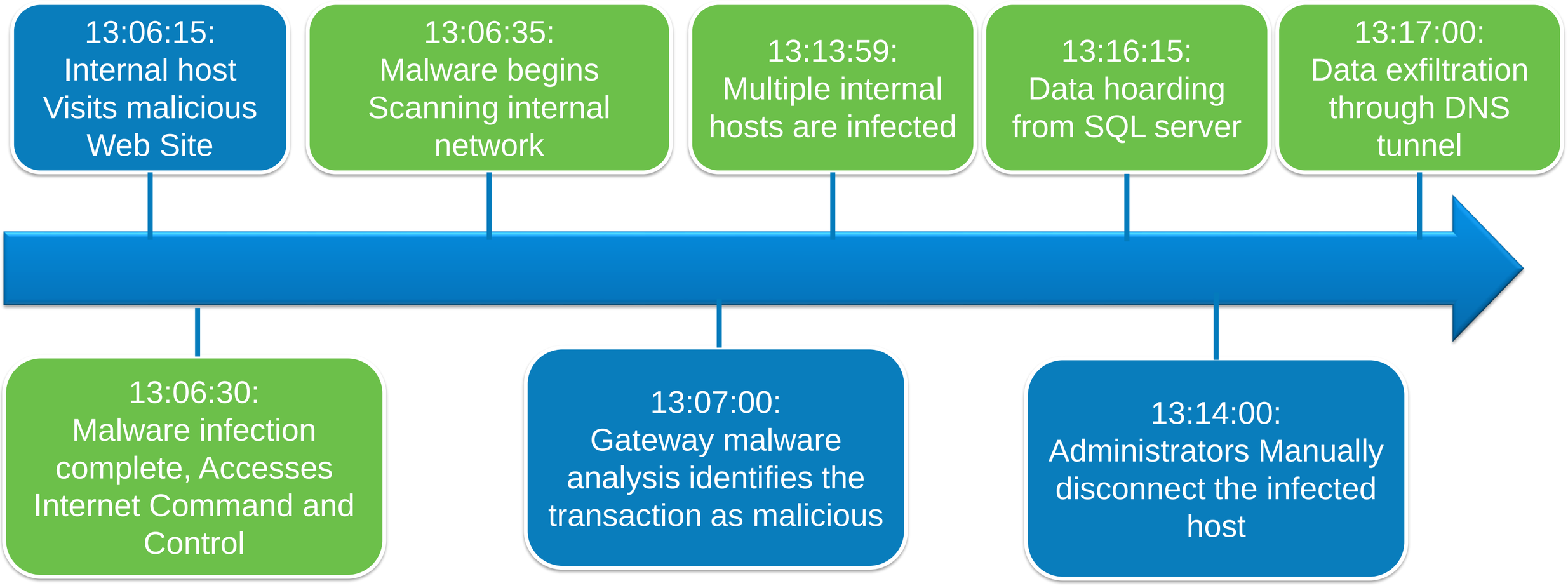
Admin Node

3 **Exploitation and Privilege Elevation**

4 **Staging and Persistence**

Timeline Security Operations Centre

IOC (Indicator of Compromise)



StealthWatch Intelligence Security Examples

Network Scanning

TCP, UDP, Port Scanning Across Multiple Hosts

Denial of Service

SYN Half Open; ICMP/UDP/Port Flood

Host Reputation Change

Inside Host Potentially Compromised

Botnet Detection

When Inside Host Talks to Outside C&C Server

Fragmentation Attack

Host Sending Abnormal # Malformed Fragments

Worm Propagation

Worm Infected Host Scans, etc.

Data Exfiltration

Large Outbound File Transfer VS. Baseline

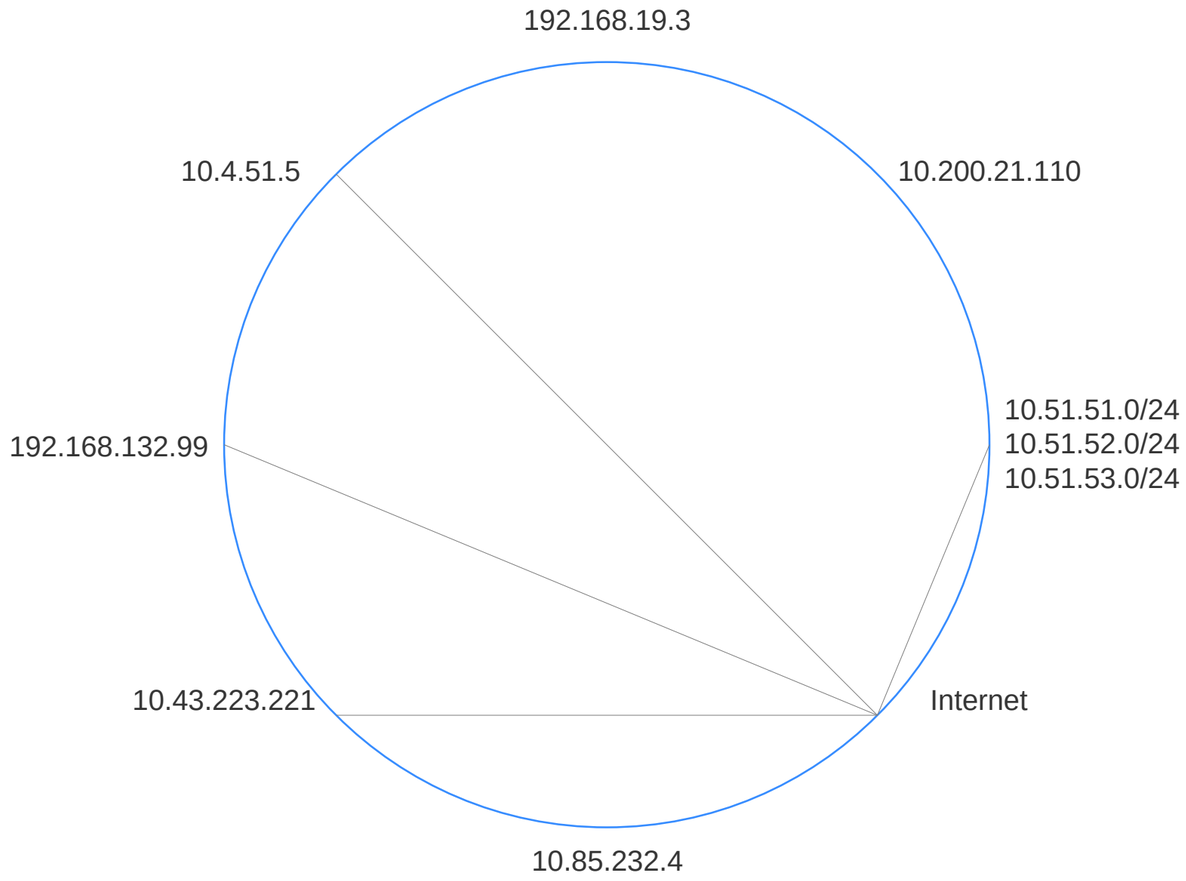
IoT Behavioral analytics

Host baselining and micro segmentation policies for M2M

Network with Only Perimeter Visibility

Many devices in your network without visibility

Visibility available for traffic transiting through perimeter



Flow adding visibility

Wired/Wireless Access Refreshes

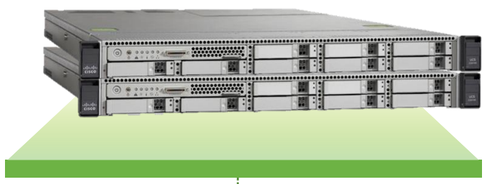
WAN/Branch

Core

DC core

Firewall

ISE

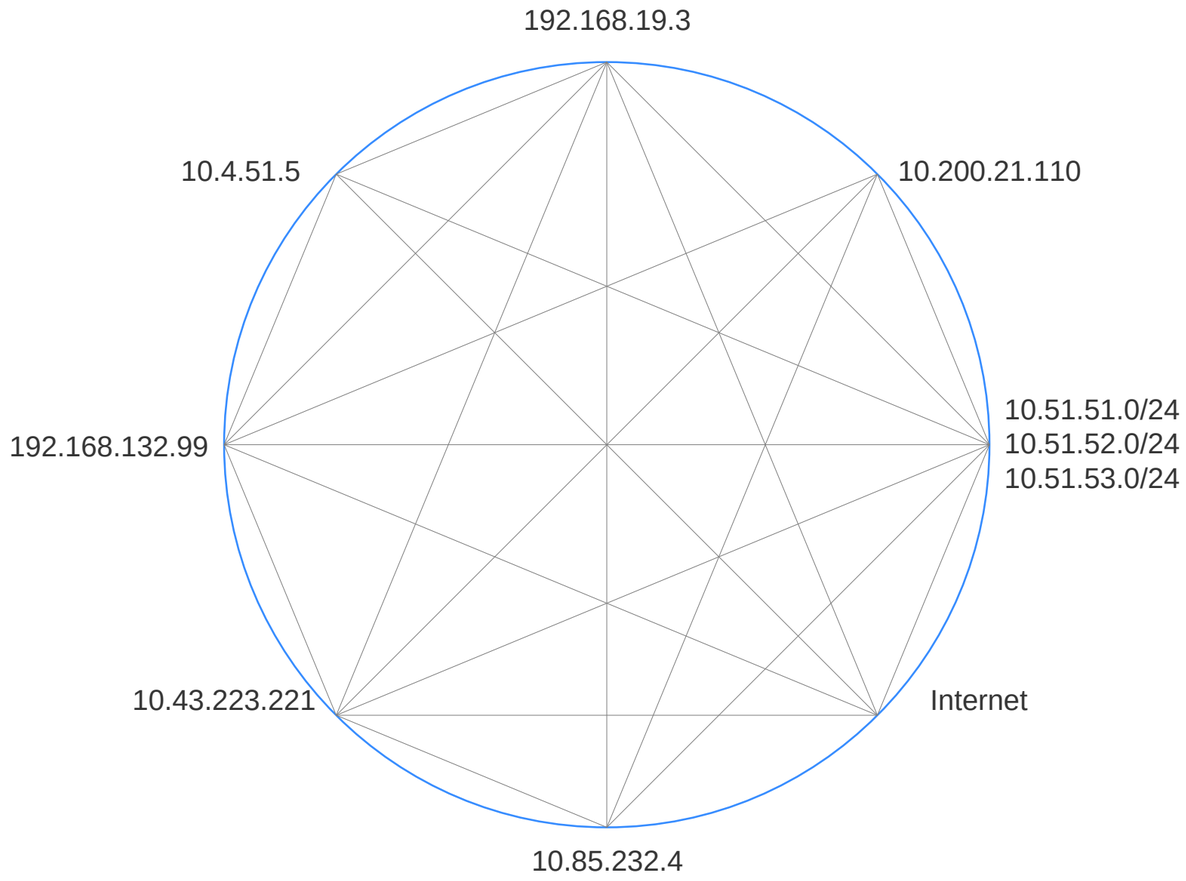


Flowsensor

Enabling Visibility Inside Your Network

Cryptic network addresses that may change constantly

Difficult to manage policy without any context



Context

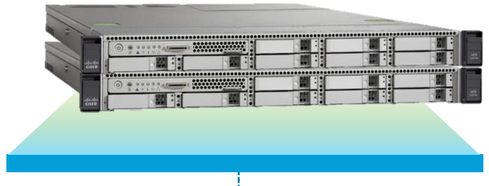
(Next Gen)
Firewall

Web proxy

Active Directory
-
Radius

Routers

Firewall

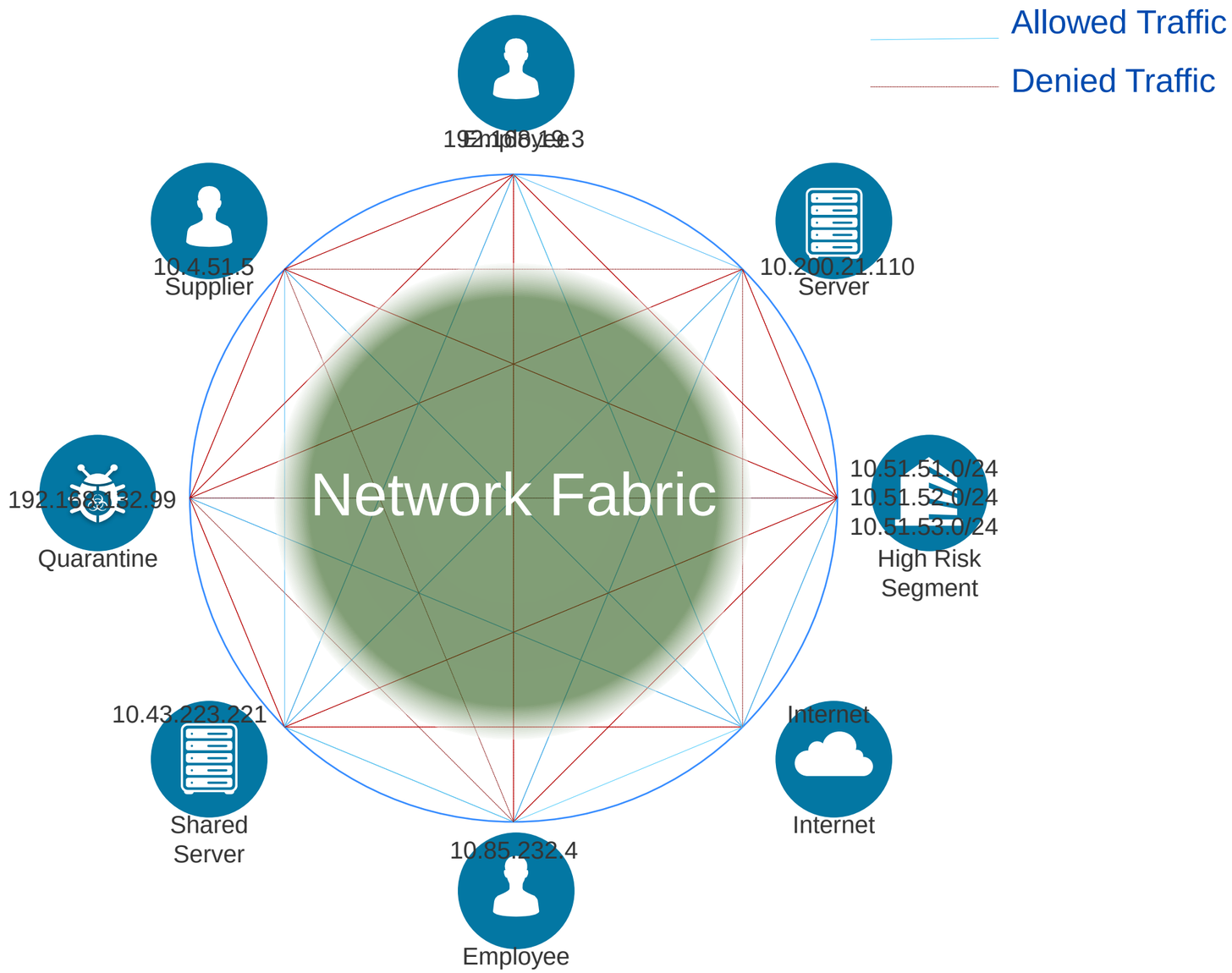


Cisco ISE
or 3d party NAC

Visibility with Context and Control

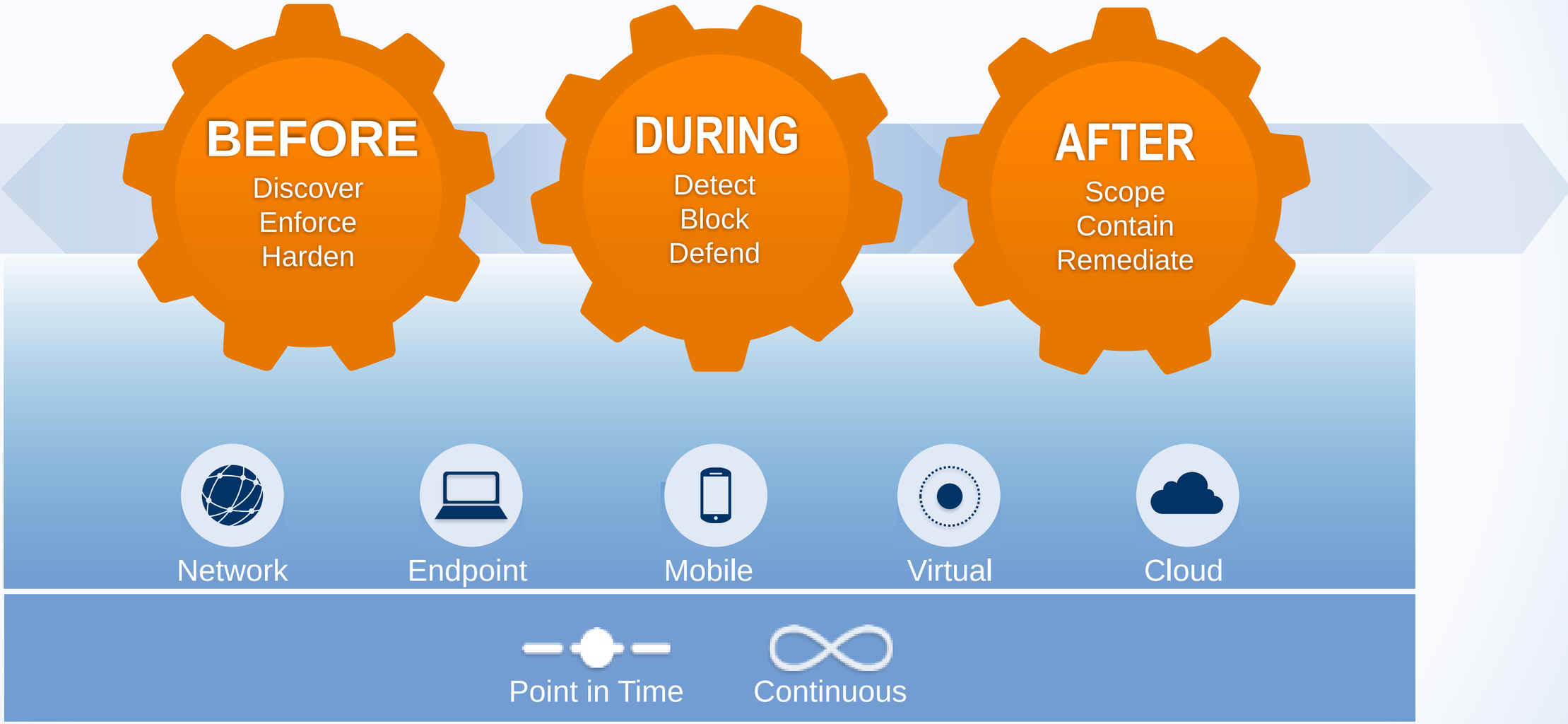
Clear understanding of traffic flow with context

Easier to create & apply policy based on such context

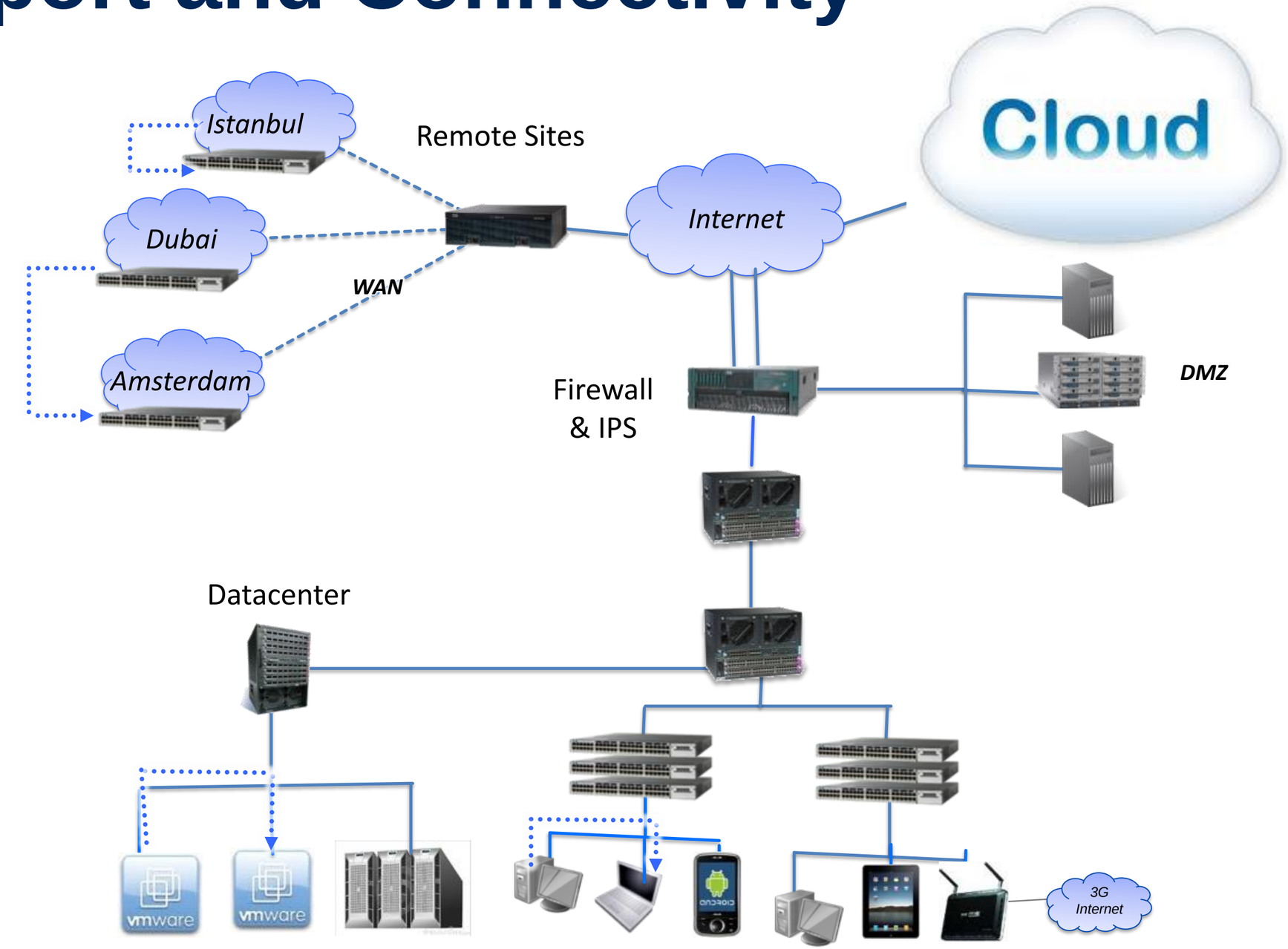


The Cisco Security Model

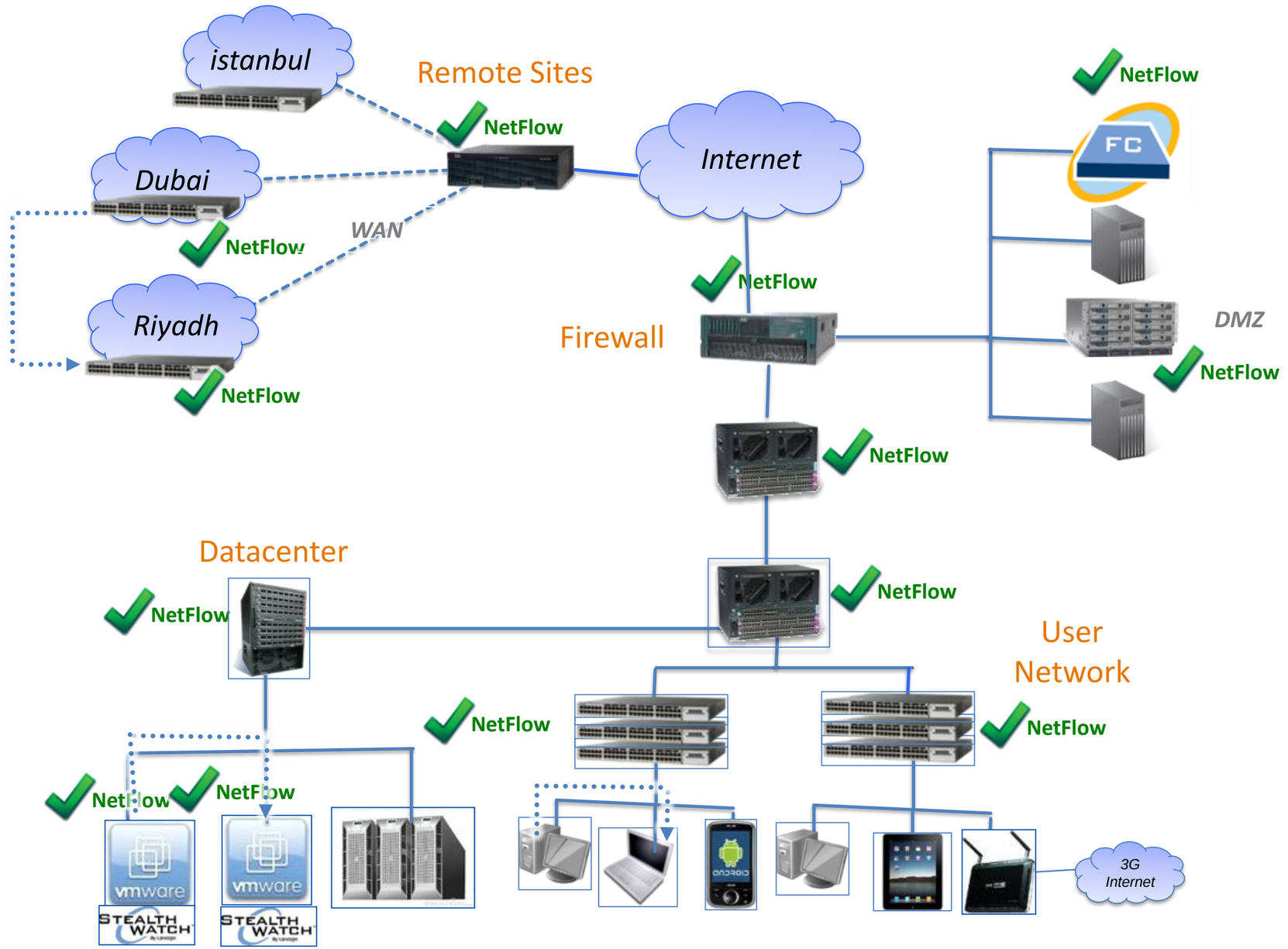
Attack Continuum



Transport and Connectivity



Network As A Sensor - StealthWatch



The Netflow/IPfix journey

Step 1
Basic Monitoring

- Host group utilization
- Interface congestion
- Top “X” reports
- Forensic logging

Step 2
Enhanced Monitoring

- RTT/SRT Tracking
- Slow Flow Alarms
- VM visibility
- User based reporting
- Policy violations
- Network mapping

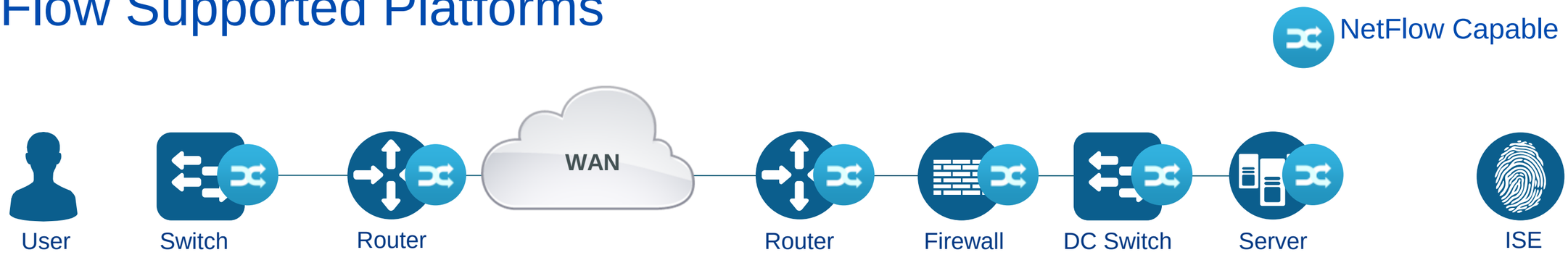
Step 3
Routine Threat Detection

- Worm propagation
- BotNet detection
- DLP on “Crown Jewels”
- Recon Detection
- DDoS Detection
- Extended storage capabilities (years not days)

Step 4
Advanced threat Detection

- Targeted attacks
- Advanced Data exfiltration Techniques
- Full Incident response

NetFlow Supported Platforms



NetFlow Exporters

Catalyst 2960-X (NetFlow Lite) - Sample Only
Catalyst 3560-X (SM-10G module only)
Catalyst 3750-X (SM-10G module only)
Catalyst 3850/3650 (FNF v9 SGT support)
Catalyst 4500E (Sup7E/7LE)
Catalyst 4500E (Sup8) (FNF v9 SGT support)
Catalyst 6500E (Sup2T) (FNF v9 SGT support)
Catalyst 6800 (FNF v9 SGT support)
Cisco ISR G2 (FNF v9 SGT support)
Cisco ISR 4000 (FNF v9 SGT support)
Cisco ASR1000 (FNF v9 SGT support)
Cisco CSR 1000v (FNF v9 SGT support)

Cisco WLC 5760 (FNF v9)
Cisco WLC 5520, 8510, 8540 (v9) *
ASA5500, 5500-X (NSEL)
Nexus 7000 (M Series I/O modules – FNF v9)
Nexus 1000v (FNF v9)
Cisco NetFlow Generation Appliance (FNF v9)
Cisco UCS VIC (VIC 1224/1240/1280/1340/1380)
Cisco AnyConnect Client (IPFIX)

Lancope

VISION TO SECURE, INTELLIGENCE TO PROTECT

StealthWatch Management Console

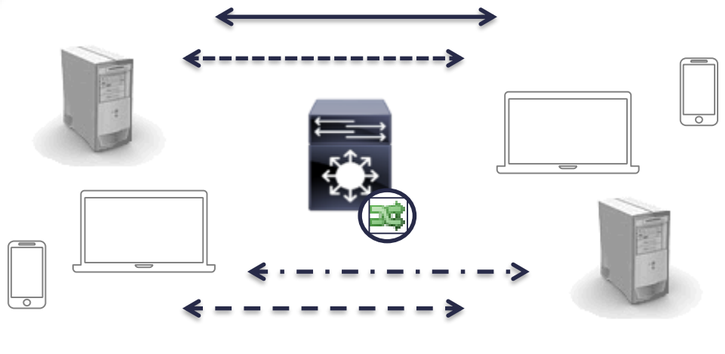
StealthWatch FlowCollector

StealthWatch FlowSensor

More Info: http://www.cisco.com/c/en/us/solutions/enterprise-networks/threat-defense/index.html

Analysis and Correlation with StealthWatch

1



Collect & Analyze Flows

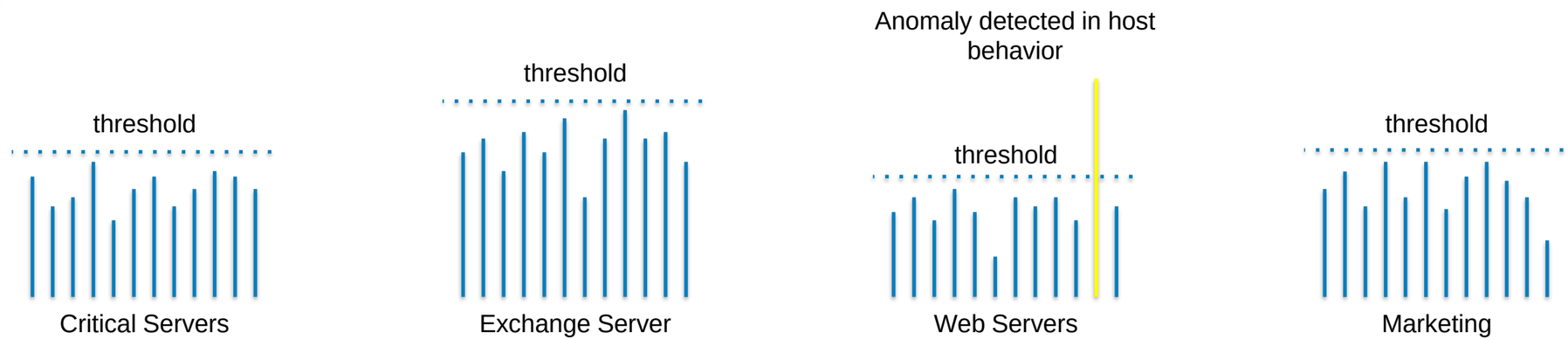
2

- # Concurrent flows
- Packets per second
- Bits per second
- New flows created
- Number of SYNs sent
- Time of day

- Number of SYNs received
- Rate of connection resets
- Duration of the flow
- Over 80+ other attributes

Establish Baseline of Behaviors

3



Alarm on Anomalies & Changes in Behavior

Behavioral and Anomaly Detection Model
Behavioral Algorithms Are Applied to Build “Security Events”

COLLECT AND ANALYZE FLOWS

SECURITY EVENTS (94 +)

Addr_Scan/tcp
Addr_Scan/udp
Bad_Flag_ACK**
Beaconing Host
Bot Command Control Server
Bot Infected Host - Attempted
Bot Infected Host - Successful
Flow_Denied
.
.
ICMP Flood
.
.
Max Flows Initiated
Max Flows Served
.
Suspect Long Flow
Suspect UDP Activity
SYN Flood

ALARM CATEGORY

- Concern
- Recon
- C&C
- Exploitation
- Data hoarding
- Exfiltration
- DDoS target

RESPONSE

- Alarm table
- Host snapshot
- Email
- Syslog / SIEM
- Mitigation

Enforcing Policy - Unwanted traffic and traffic types

Completely customizable rules

For instance:

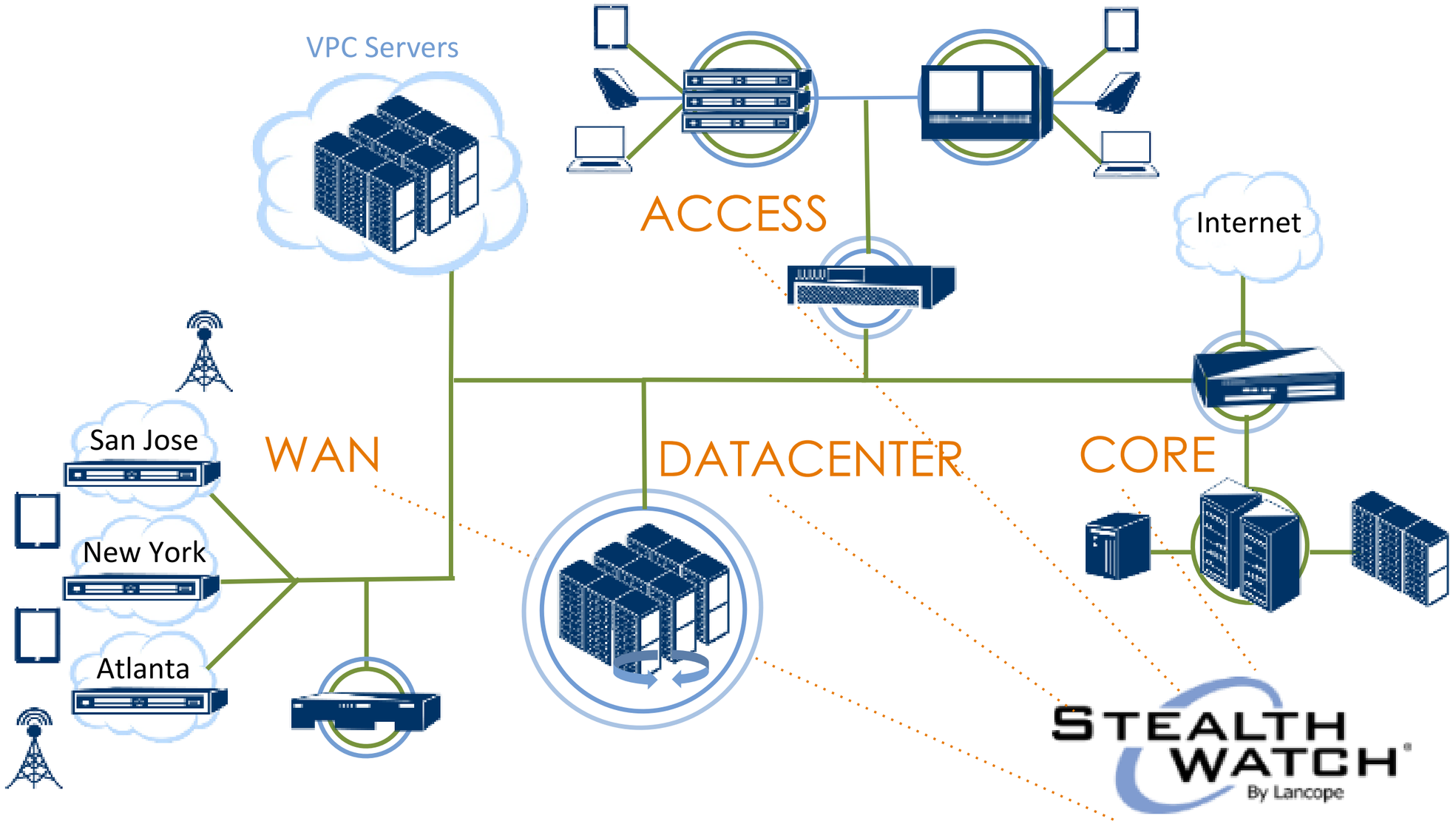
FTP	unencrypted file transfer
Telnet	unencrypted management traffic, i.e. firewall rule auditing
BitTorrent	consumes large amounts of bandwidth and a source of malware)
Rouge DHCP	can start “blackholing” traffic

Traffic between confidential servers and the internet, between SCADA and LAN

Outgoing traffic from certain areas of the NW destined for certain countries (Israel, China or Russia for instance)

Network visibility and NPM

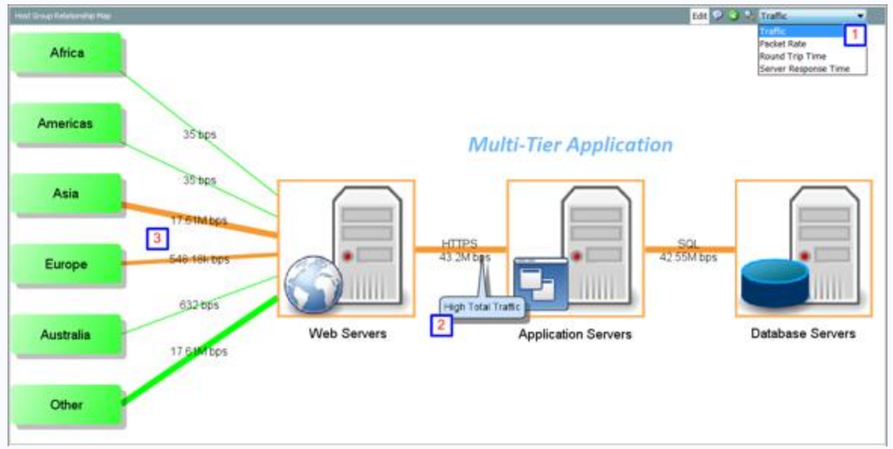
Internal Visibility from User to Edge to Access to core to Application

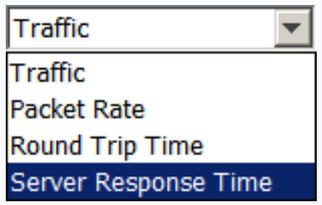


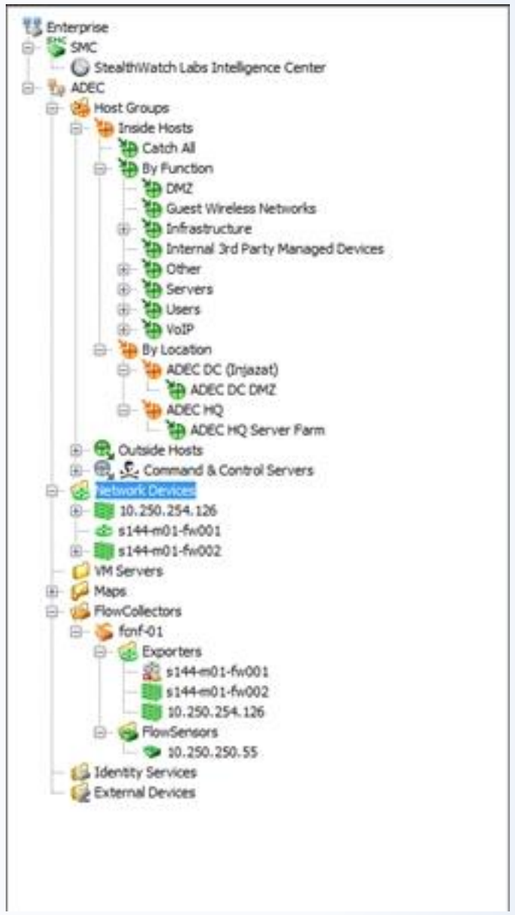
Network vs Security vs Application/Server

Server response time (SRT)?
How long is the server taking to respond to user requests?

Which user community is affected more than others?

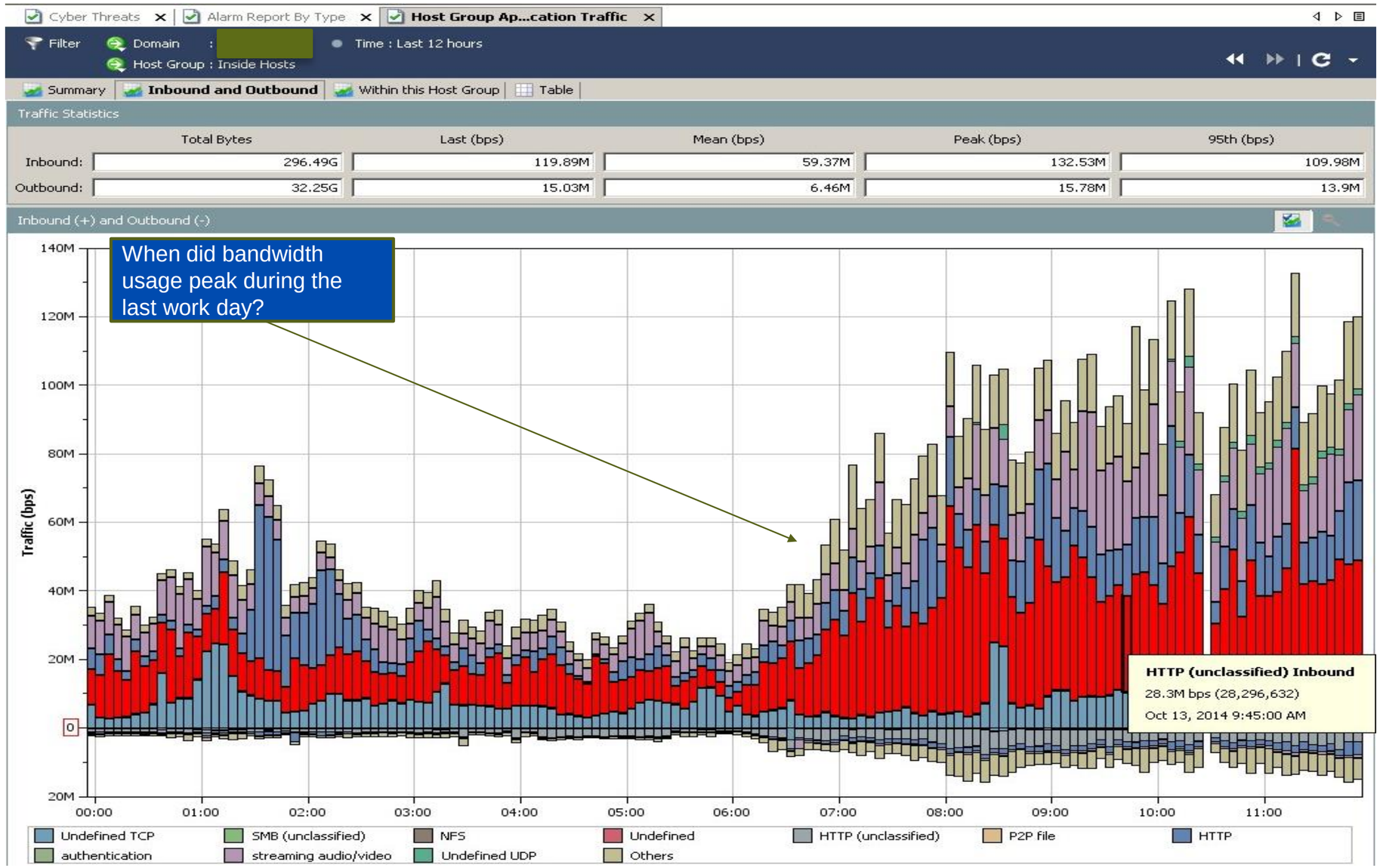






Lancope

Traffic analysis – what is causing the issue
(host, application, protocol, user etc)



Network as an Enforcer

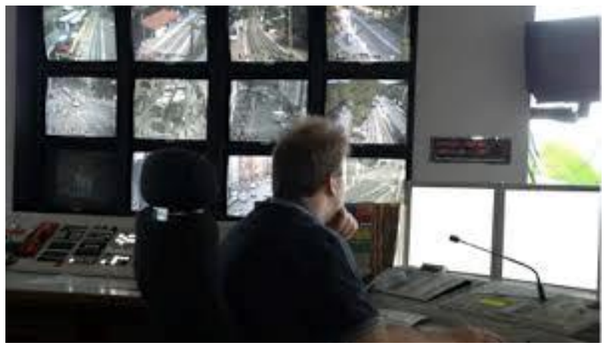
StealthWatch ISE integration

(can be done with 3d party NAC as well)

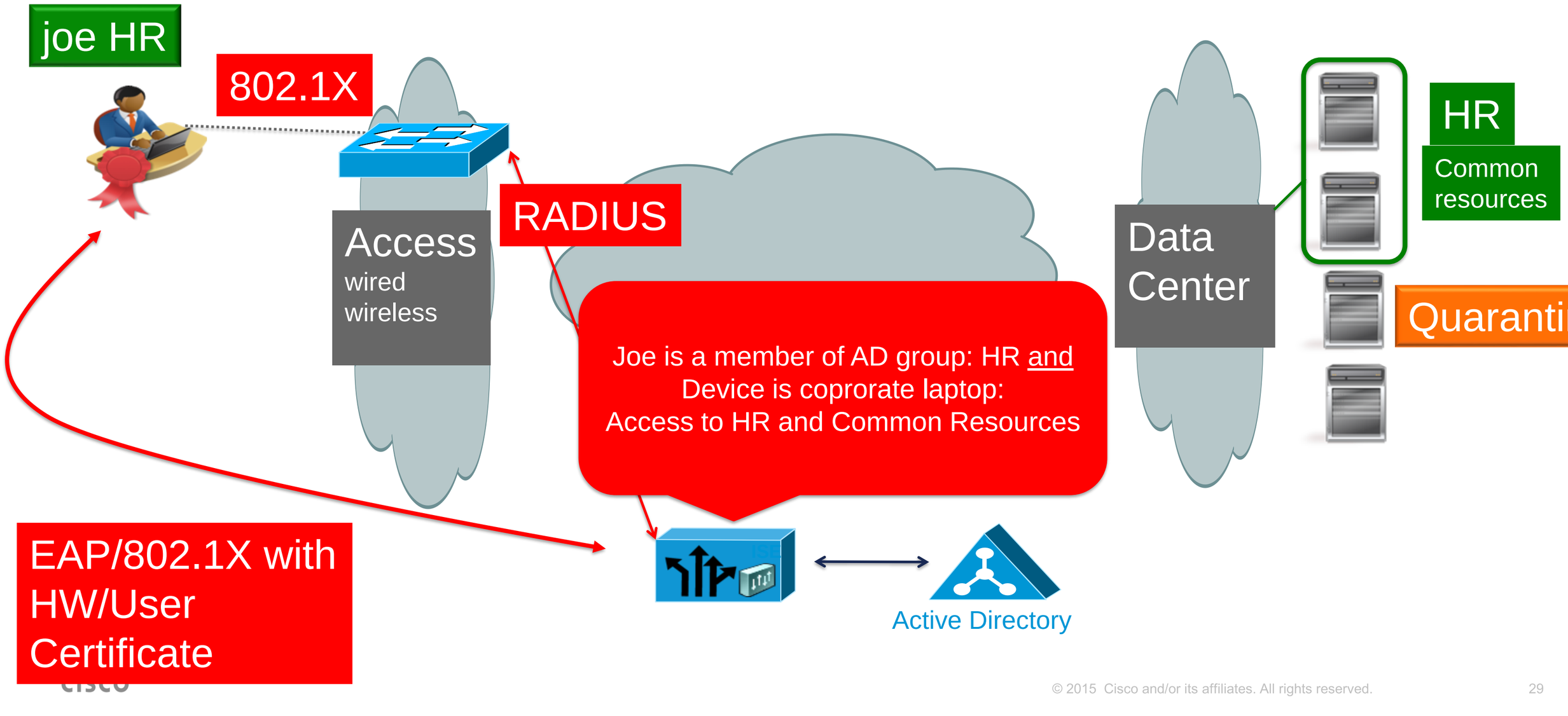
ISE integration – Network as an Enforcer

- ISE provides **Access Control**
  i.e. card readers for a building

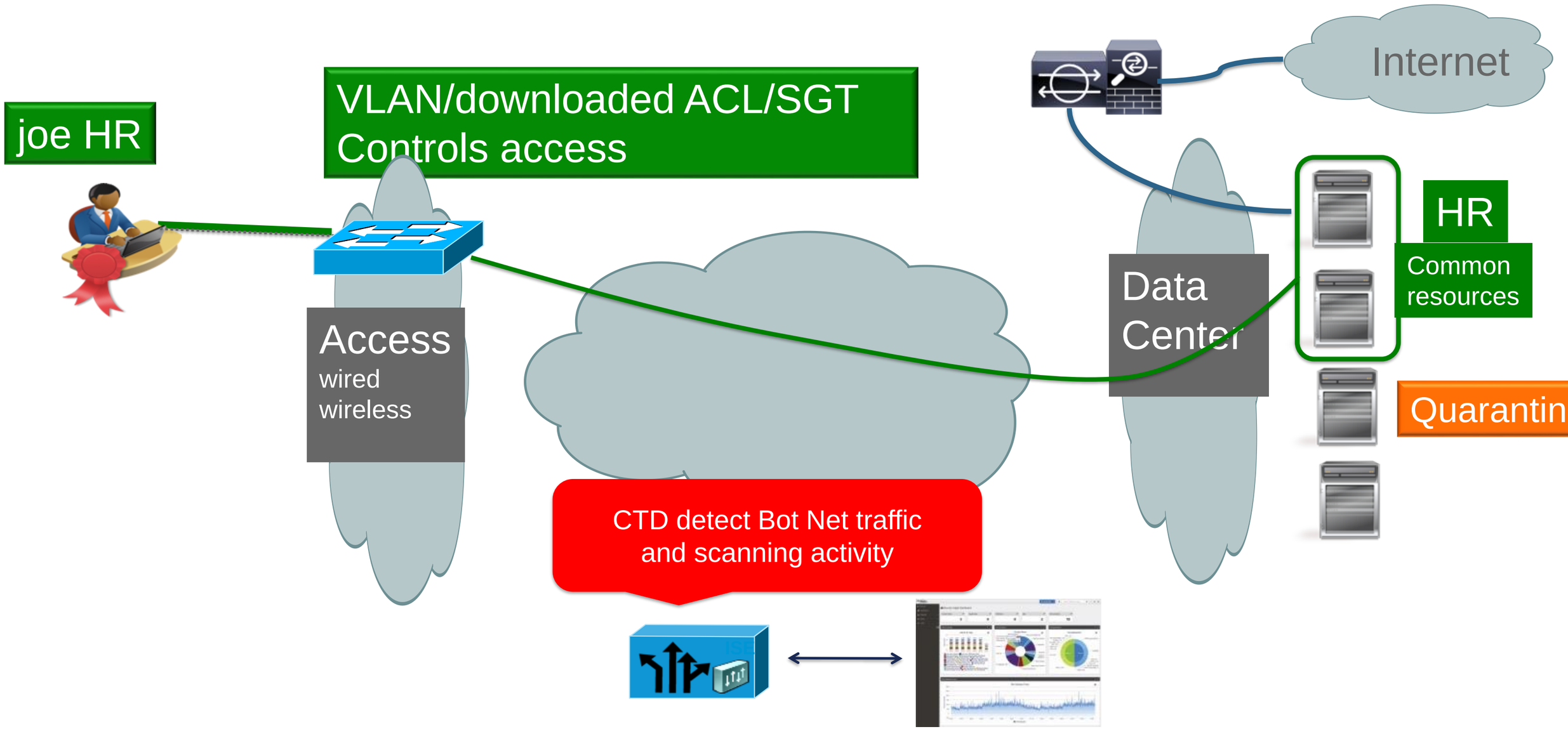
- NaaS/E adds **Automated Behavior Analytics**
  i.e. cameras watching and intelligence analyzing



Standard ISE implementation, context based access

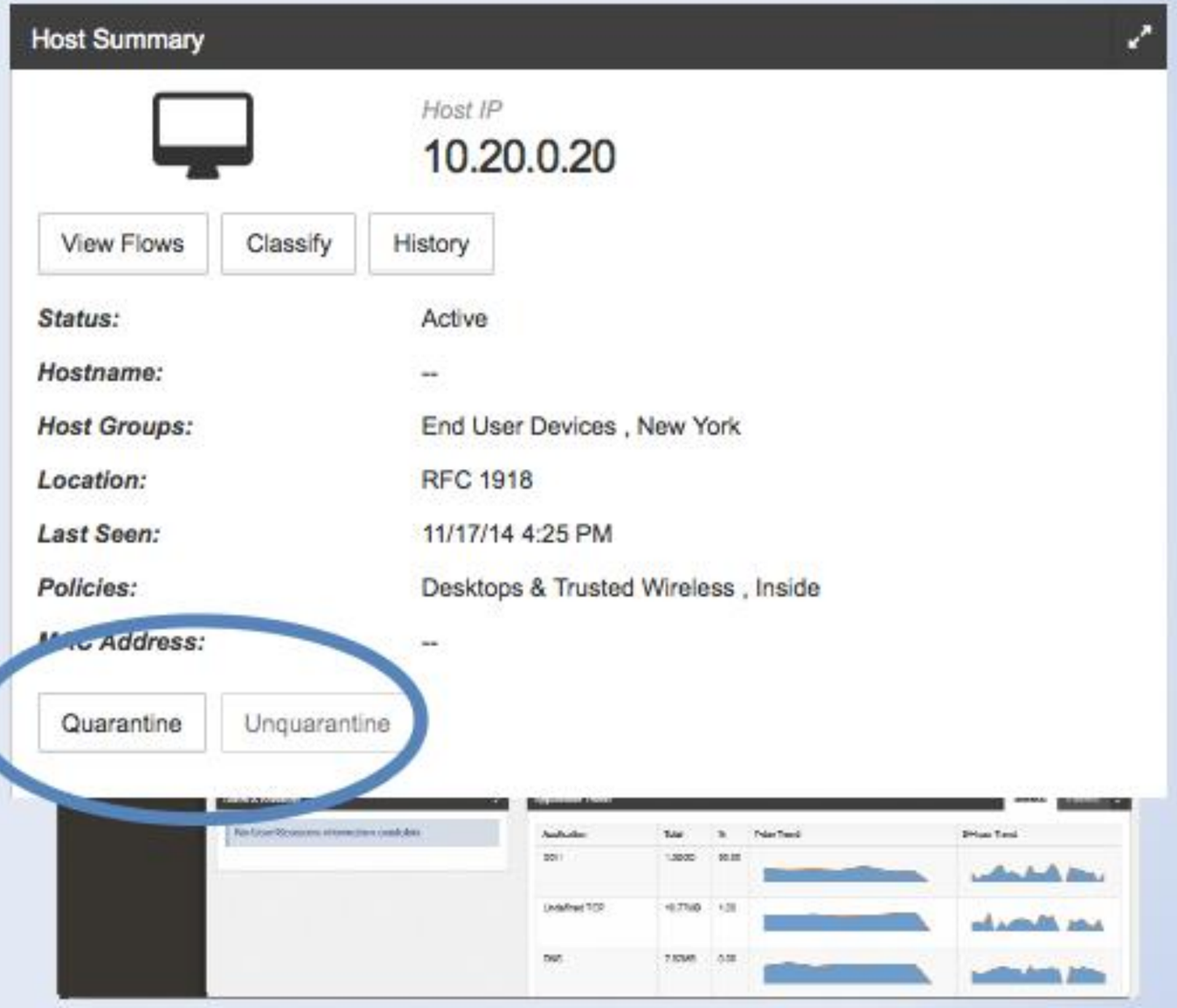


Network as an Enforces (NaaE) using ISE



Cisco ISE 1.3 Integration

- StealthWatch will now utilize the Cisco pxGrid API to initiate a Quarantine action
- Through the StealthWatch interface a quarantine action can be initiated from the host dashboard



Lancope

NaaE - quarantine access

VLAN/downloaded ACL/SGT
Controls access only to
Quarantine VLAN

joe HR

Access
wired
wireless

Internet

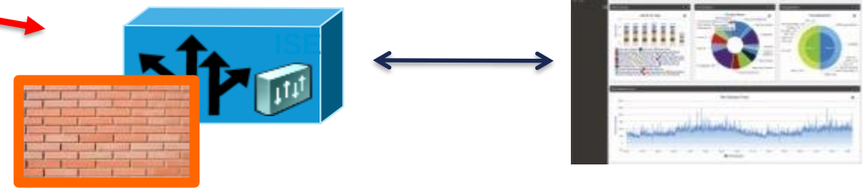
Data
Center

HR
Common
resources

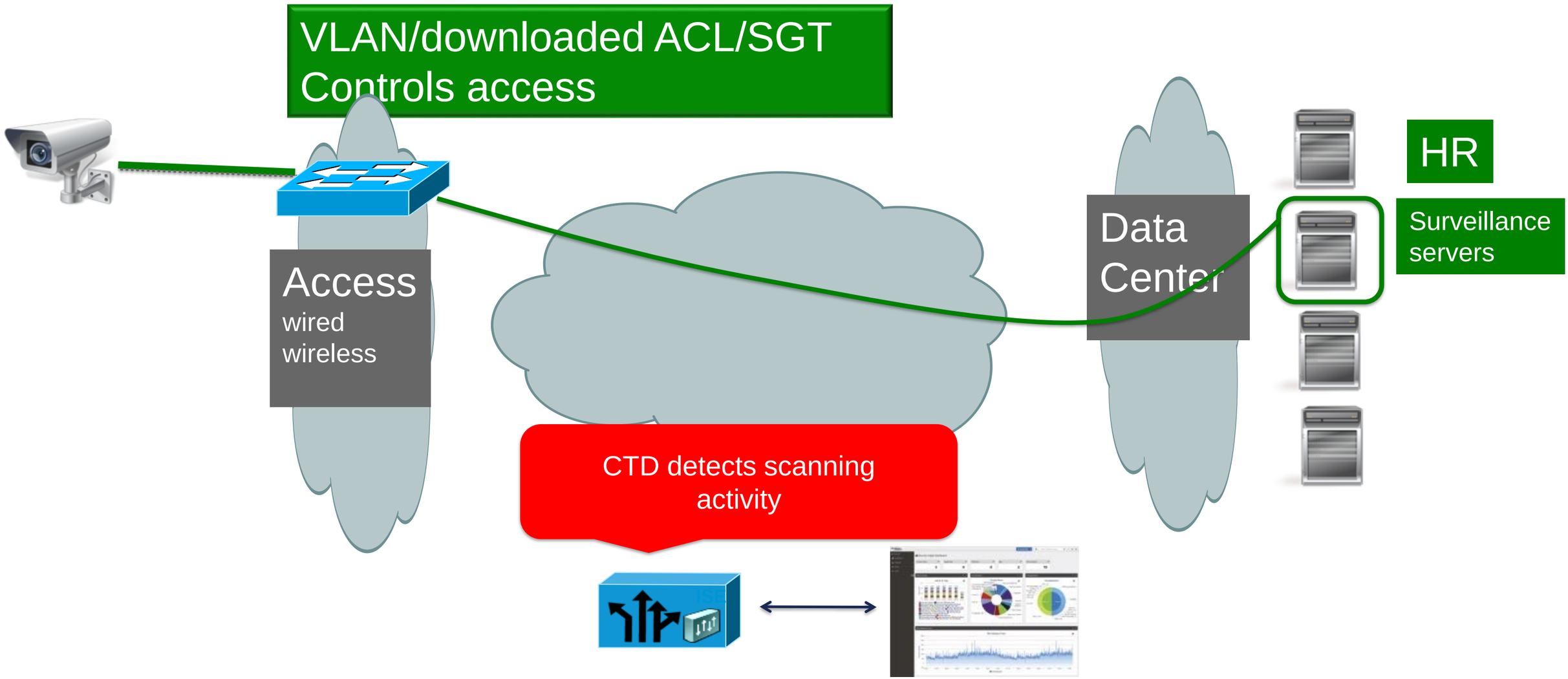
Quarantine

ISE receives input from CTD
to change security status of joe

Send CoA command to
the Switch/WLC



IoT example – PCAP and IPS



IoT example – PCAP and IPS

VLAN/downloaded ACL/SGT
Controls access only to Quarantine VLAN

Access
wired
wireless

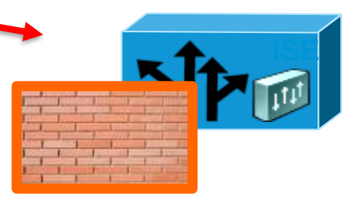
Data Center

HR

Surveillance servers

ISE receives input from CTD to change security status of Surveillance Camera

Send CoA command to the Switch/WLC



Packet Analyzer

Strengthen your threat investigations

Purpose-built on-prem appliance for robust forensics investigation

Captures all frames with real-time 4 x 1 GE and 2 x 10 GE network performance

Stores relevant packet data discretely up to 42 TB

Accelerates incident response based on targeted analysis of packets

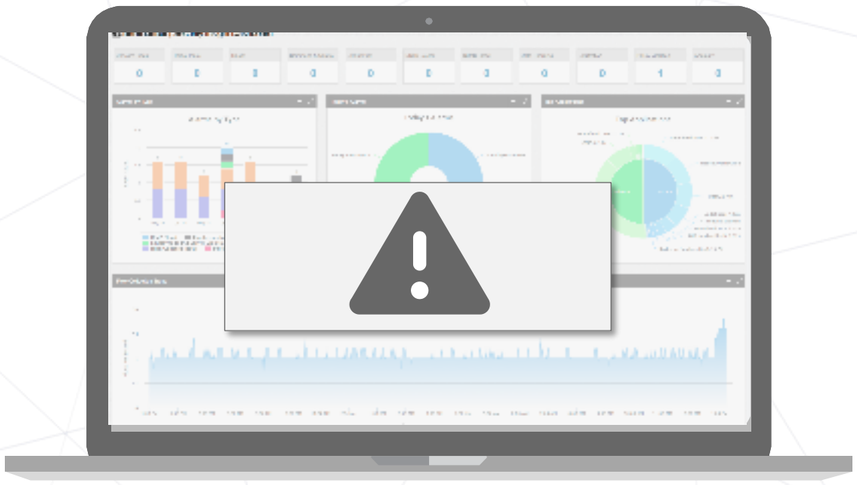
Answers the how, what, and where your network has been affected

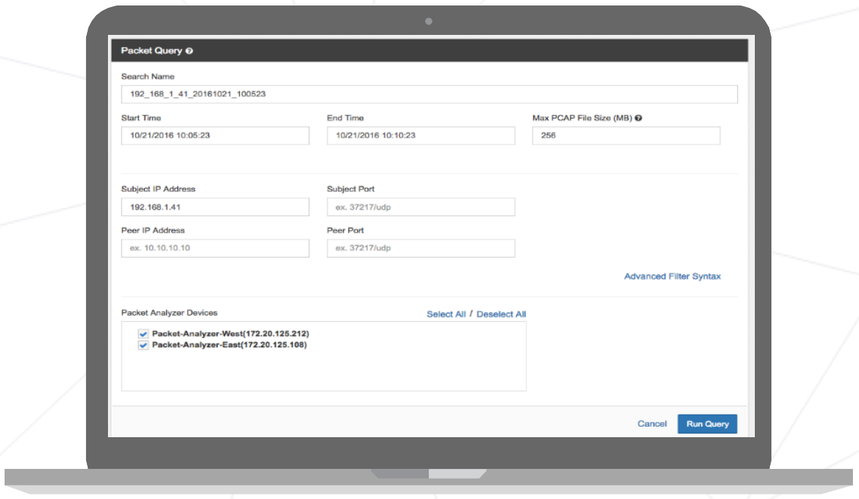
Reduce time to resolution with precision search

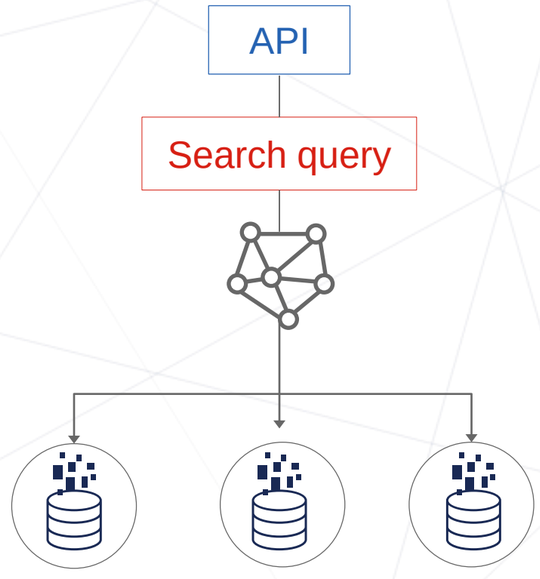
1 Alarm sent to SMC alerting you to suspicious activity

2 Type search query in SMC and select which PAs to search

3 Using appliance API, search query is sent to selected PAs

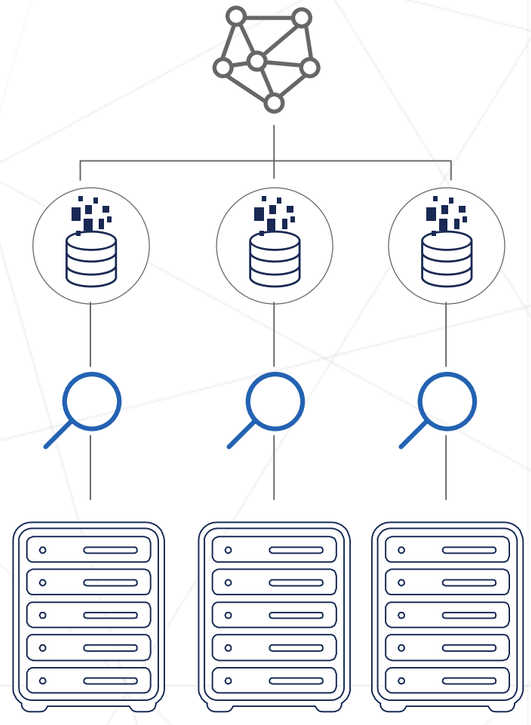




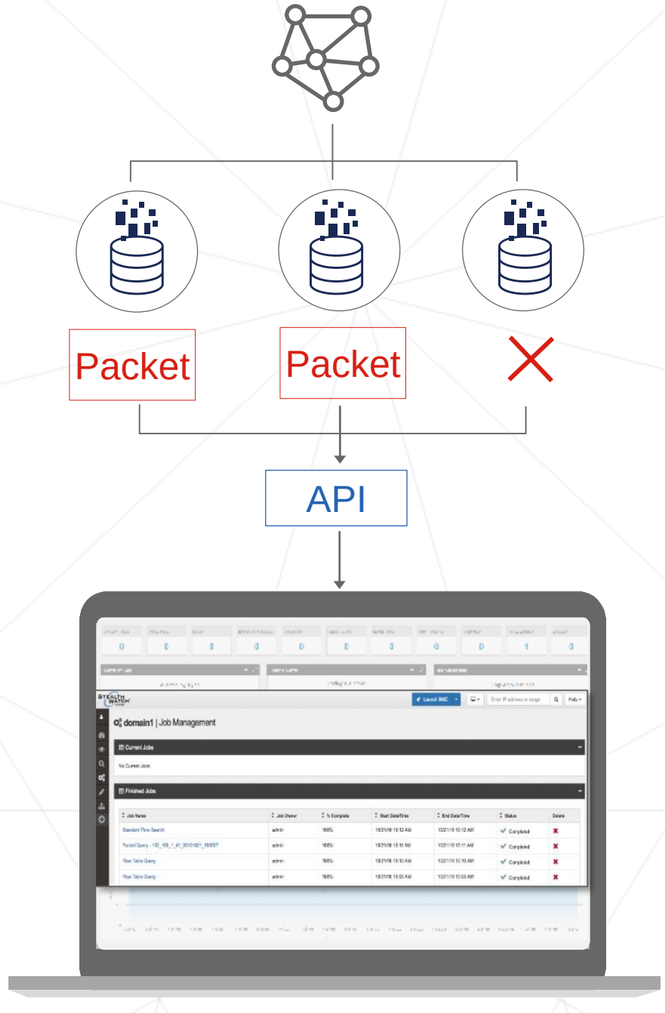


Reduce time to resolution with precision search

4 PAs search in parallel for packets matching search query criteria



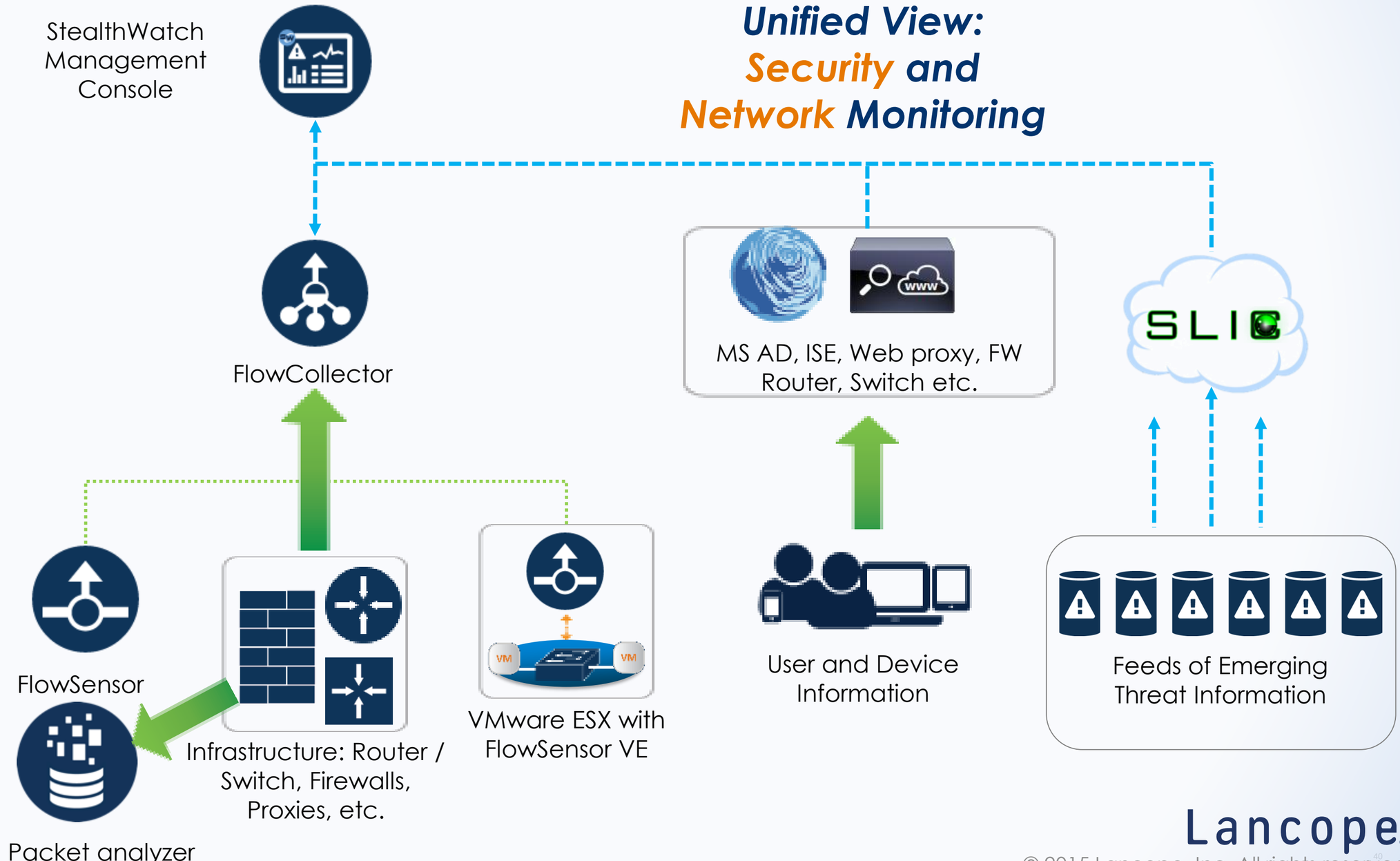
5 PAs retrieve packets and use appliance API to send packets to SMC



6 Retrieved packets are now available to review in SMC

Architecture and Summary

Architecture Detail



Summary StealthWatch

- Move close to 1:1 network conversation visibility and 100% coverage using your existing network.

- Strong network performance monitoring solutions

The Attack and Defense continuum:

- Before: Discover and manage network segmentation and policy violations

- During: Increased visibility provides threat detection through algorithm based behavioral detection

  Attackers (CI), Targets (TI), Data movement (DH/DE)

  Context + Lancope = Rich context and Enforcement capabilities

- After: Forensic capabilities which eliminates blind spots and stretches years back. Trace every step of an attack, not only the initial infection

Working with StealthWatch

An “Edward Snowden example”

ALERT: Insider Threat

Scenario: An internal user is stealing data!

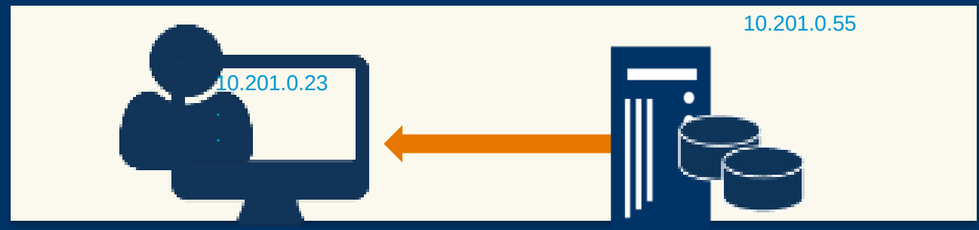
The user could be a:

- Disgruntled employee
- Person about to leave the company
- Person with privileged credentials
- Person stealing and selling trade secrets

Security events have triggered indicating a user is connecting to a terminal server, collecting data from a sensitive database, and tunneling the traffic out of the network using P2P through UDP port 53 (DNS port).

1. Internal user connects to Terminal Server

2. Terminal server used to collect sensitive data from within the same subnet inside the datacenter.



3. Terminal server used to encrypt data and tunnel through DNS port to an upload server

Lancope

Insider Threat Demo (Data Loss)

Launch SMC | enter IP address or range

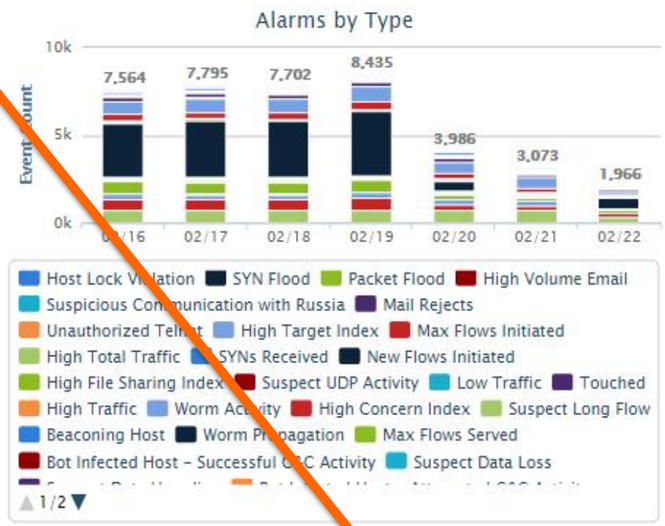
Joe Buchanan

- Dashboard
- Network
  - Host
  - User
- Flows
- Tools

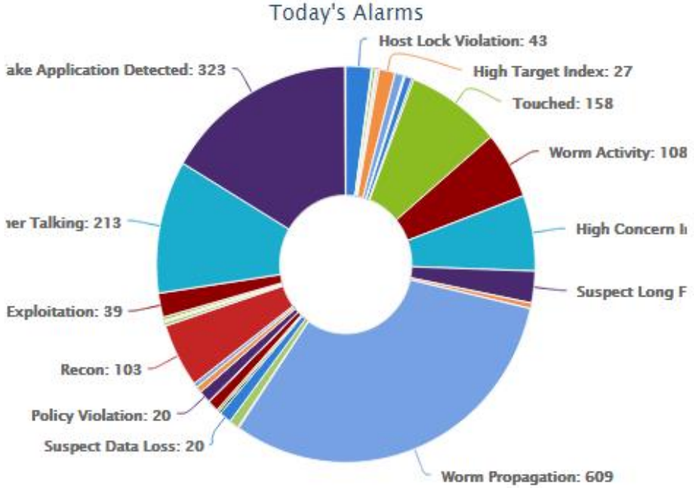
Security Insight Dashboard

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	0	0	0	0	0	0	2	2	0	0

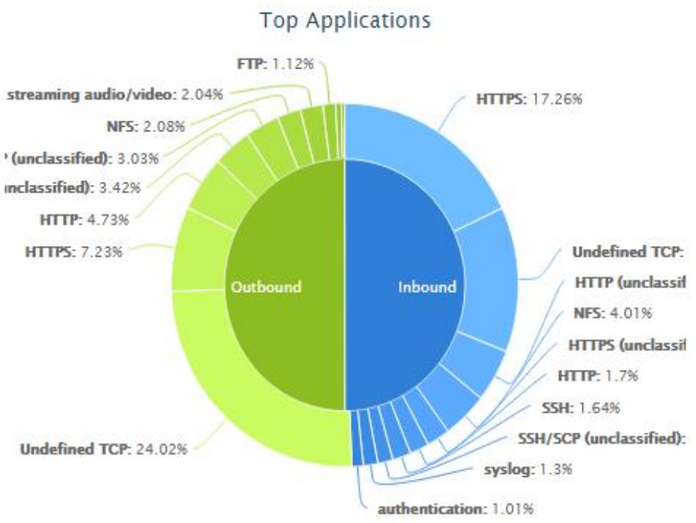
Alarms by Type



Today's Alarms

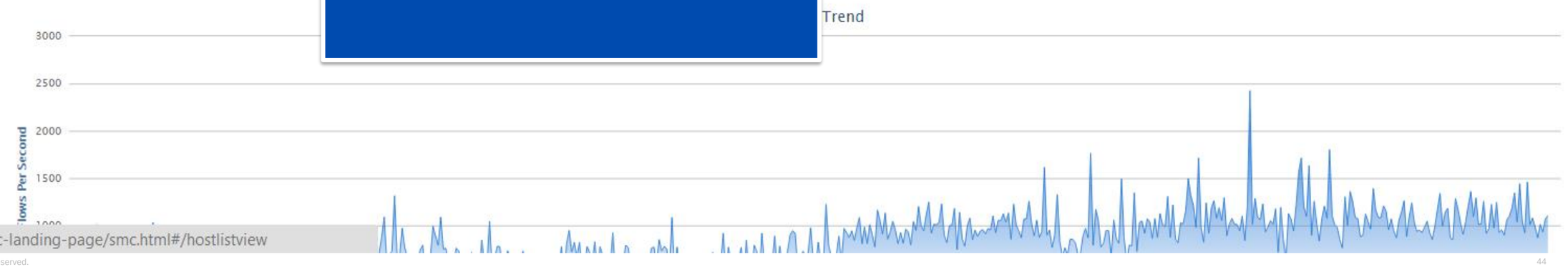


Top Applications



List of All hosts

Flow Collection Trend



https://smcreplica.lancope.com/lc-landing-page/smc.html#/hostlistview

STEALTH WATCH

Launch SMC | enter IP address or range

Joe Buchanan

- Dashboard
- Network
  - Host
  - User
- Flows
- Tools

Hosts (2000)

Alarms

Index/Severity

Host Group

IP/Host name

Hosts

Sorted by overall severity

Data Hoarding | A source or target host within a network has downloaded an unusual amount of data from one or more hosts.

Host Address	Host Name	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Location	Host Groups
10.201.3.78		10%		2%	2								RFC 1918	Sales and Marketing, Atlanta, Desktops
10.201.0.55	database-server.								1,176,553%				RFC 1918	Datacenter, Database Servers
10.201.0.23	terminal-server.	1%		3%					75,735%				RFC 1918	Terminal Server, Datacenter
10.201.5.25		2,799%		6%		65%							RFC 1918	Infrastructure
10.10.101.43		1,241%		1%		37%							RFC 1918	New York, Desktops
10.10.30.23		889%		1%		26%							RFC 1918	New York, Desktops
10.10.101.24		742%		21%		1%							RFC 1918	New York, Desktops
10.202.4.71		3%		715%									RFC 1918	Engineering, Boston
10.10.101.118		329%		1%		8%							RFC 1918	New York, Desktops
10.10.101.27		302%		3%		7%							RFC 1918	New York, Desktops
10.201.3.21	spare2-2-13-15.lancope.local.	237%		1%		23%							RFC 1918	Sales and Marketing, Atlanta, Infrastructure, Desktops

Recon (247)
Concern Index (212)
Exploitation (26)
Target Index (10)
Command & Control (6)
Data Hoarding (2)
Anomaly (1)
Exfiltration (0)
DDoS Source (0)
DDoS Target (0)
Policy Violation (0)
Select Multiple

Host Groups

Inside Hosts (3383)

Locations

RFC 1918 (1665)
United States (304)
Unknown (31)
Select Multiple

Alarms

Host information

User history

Device Type

34G of SQL downloaded By our terminal server

Ongoing traffic
Let's look at external as well

Launch SMC | enter IP address or range

Joe Buchanan

- Dashboard
- Network
  - Host
  - User
- Flows
- Tools

Host Report for 10.201.0.23

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	0	0	0	0	0	0	2	2	0	0

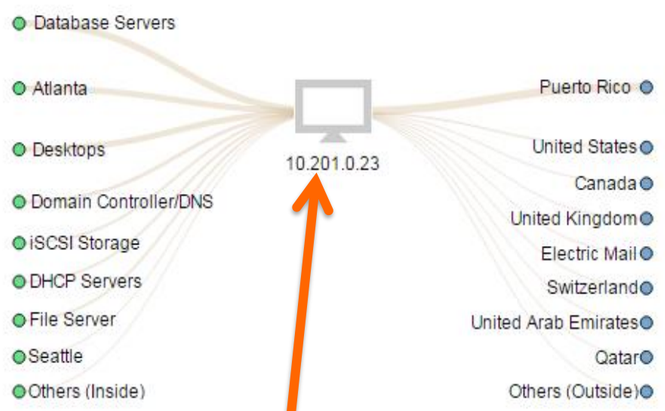
Host Summary

Host IP
10.201.0.23

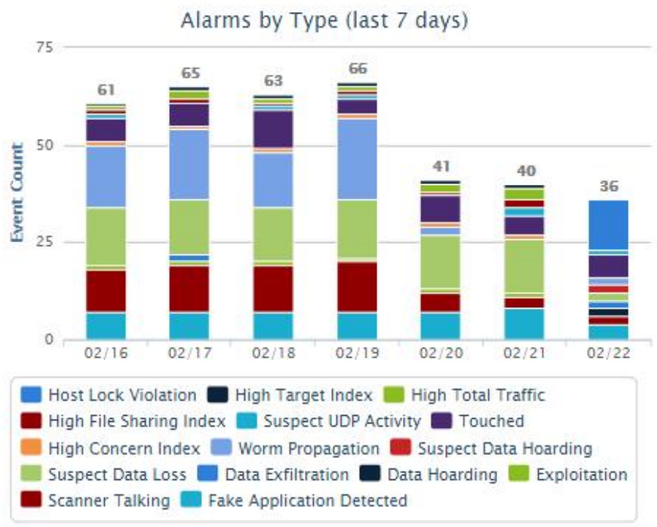
View Flows | Classify | History

Status:	Active
Hostname:	terminal-server
Host Groups:	Terminal Server, Datacenter
Location:	RFC 1918
Last Seen:	2/22/15 1:46 PM
Policies:	High Target Index Supress, Inside, Lancope Datacenter Policy
MAC Address:	00:26:b9:9f:aa:66 *(Dell Inc)*

Traffic by Peer Host Group



Alarms by Type



Users & Sessions

Mac Address: 00:26:b9:9f:aa:66 **Mac Vendor:** Dell Inc **Device Type:** Windows7 Workstation

User	Start	End
edward	2/22/15 5:06 AM	2/22/15 5:33 AM
edward	2/22/15 5:46 AM	2/22/15 9:06 AM

Application Traffic

Internal | External

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
Undefine...	41.89GB	31.00	40.55GB		1.33GB		
SQL	34.59GB	26.00	298.92MB		34.29GB		
NFS	26.92GB	20.00	513.24MB		26.42GB		

STEALTH WATCH

Launch SMC | 10.201.3.18

Joe Buchanan

- Dashboard
- Network
  - Host
  - User
- Flows
- Tools

Host Report for 10.201.0.23

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	0	0	0	0	0	0	1	0	0	0

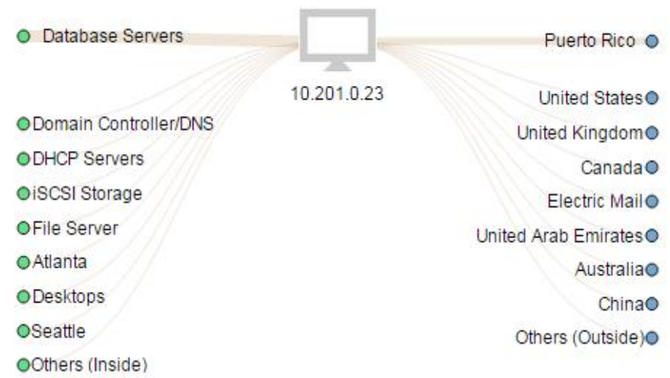
Host Summary

Host IP
10.201.0.23

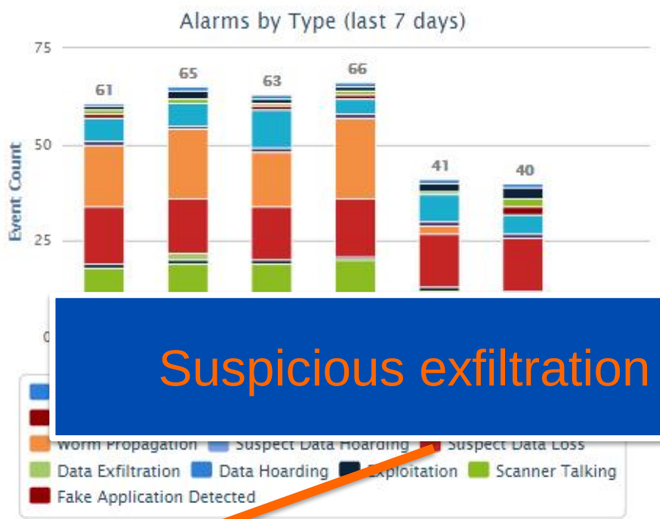
View Flows | Classify | History

Status:	Active
Hostname:	terminal-server
Host Groups:	Terminal Server, Datacenter
Location:	RFC 1918
Last Seen:	2/22/15 12:58 AM
Policies:	High Target Index Supress, Inside, Lancope Datacenter Policy
MAC Address:	00:26:b9:9f:aa:66 *(Dell Inc)*

Traffic by Peer Host Group



Alarms by Type



Suspicious exfiltration

Users & Sessions

Mac Address: 00:26:b9:9f:aa:66 **Mac Vendor:** Dell Inc **Device Type:** Windows7 Workstation

User	Start	End
edward	2/22/15 5:06 AM	2/22/15 5:33 AM
edward	2/22/15 5:46 AM	2/22/15 9:06 AM

Application Traffic

Internal | External

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
P2P file	2.96GB	60.00	2.96GB		0B		
HTTPS	1.12GB	23.00	799.63MB		348.06MB		
HTTPS (u...	569.45MB	11.00	443.04MB		126.41MB		

Detailed report
flow for flow

P2P traffic to
Puerto Rico

STEALTH WATCH

Joe Buchanan

- Dashboard
- Network
  - Host
  - User
- Flows
- Tools

10.201.3.18

Flows (118)

Actions

- Save Results
- Save Query
- Clone Query
- Export as .CSV

Current Filters

No Filters Selected

Clear All

Filter Results By:

Search Subject

Host Groups

Inside Hosts (236)

Locations

RFC 1918 (118)

Select Multiple

Port

1 - 12437 (78)
12438 - 24874 (1)
24875 - 37311 (1)
37312 - 49748 (22)
49749 - 62187 (4)

Select Multiple

Protocol

TCP (101)
ICMP (12)
UDP (5)

Flow Query Results

Duration	Search Subject	Port	Traffic Summary	Port	Peer
Start: 02/22 - 12:54:16 AM End: 02/22 - 12:57:47 AM Duration: 3m 31s	10.201.0.23 RFC 1918 terminal-server 00:06:0a:c9:00:17 View Details	32393/UDP	302.73MB | 221.14K packets → P2P file ← 0B | 0 packets	53/UDP	74.213.99.97 Puerto Rico
Start: 02/22 - 12:55:16 AM End: 02/22 - 12:57:29 AM Duration: 2m 13s	10.201.0.23 RFC 1918 terminal-server 00:06:0a:c9:00:17 View Details	443/TCP	11.69MB | 8.93K packets → HTTPS ← 299.55KB | 5.32K packets	46087/TCP	178.239.84.64 United Kingdom
Start: 02/22 - 12:54:16 AM End: 02/22 - 12:57:59 AM Duration: 3m 43s	10.201.0.23 RFC 1918 terminal-server 00:06:0a:c9:00:17 View Details	10839/TCP	493.68KB | 718 packets → authentication ← 1.01MB | 1.16K packets	3268/TCP	10.201.0.15 RFC 1918 lchqsvr01.lancope.local 00:22:19:93:07:b4
Start: 02/22 - 12:54:16 AM End: 02/22 - 12:57:59 AM Duration: 3m 43s	10.201.0.23 RFC 1918 terminal-server 00:06:0a:c9:00:17 View Details	10860/TCP	520.15KB | 730 packets → authentication ← 567.6KB | 536 packets	3268/TCP	10.201.0.16 RFC 1918 lchqsvr02.lancope.local 00:0c:29:41:3c:56
Start: 02/22 - 12:54:16 AM End: 02/22 - 12:57:47 AM Duration: 3m 31s	10.201.0.23 RFC 1918 terminal-server 00:06:0a:c9:00:17 View Details	443/TCP	119.58KB | 580 packets → HTTPS ← 347.17KB | 638 packets	60105/TCP	12.177.140.2 United States
Start: 02/22 - 12:54:16 AM End: 02/22 - 12:57:48 AM Duration: 3m 32s	10.201.0.23 RFC 1918 terminal-server 00:06:0a:c9:00:17	41463/TCP	268.14KB | 800 packets → Undefined TCP	3332/TCP	10.201.0.41 RFC 1918 lchqbes02.lancope.local
Start: 02/22 - 12:54:16 AM End: 02/22 - 12:57:59 AM Duration: 3m 43s	10.201.0.23 RFC 1918 terminal-server 00:06:0a:c9:00:17 View Details	389/TCP	1.94MB | 1.9K packets	389/TCP	10.201.0.16 RFC 1918 lchqsvr02.lancope.local 00:0c:29:41:3c:56

Thank you.