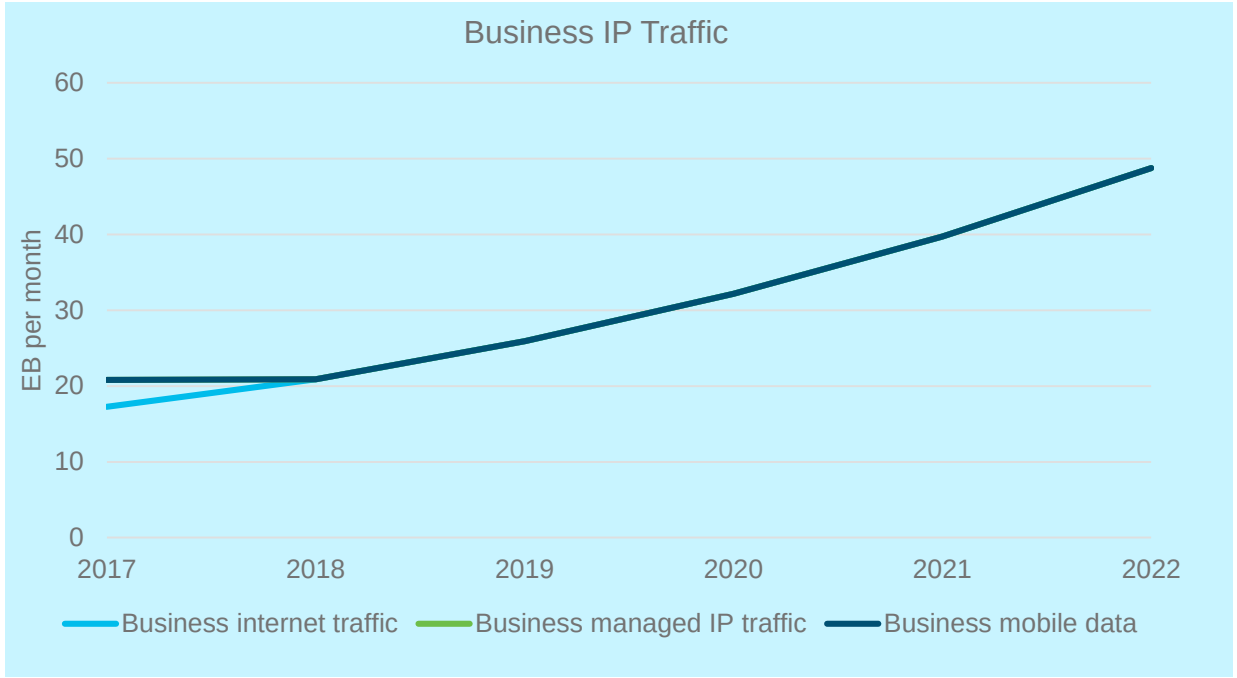
Threat Prevention based on Network Visibility & Behavioral Analytics

Luc Billot
Cyber Security Technical Architect - Cisco
April 2019

What if …..

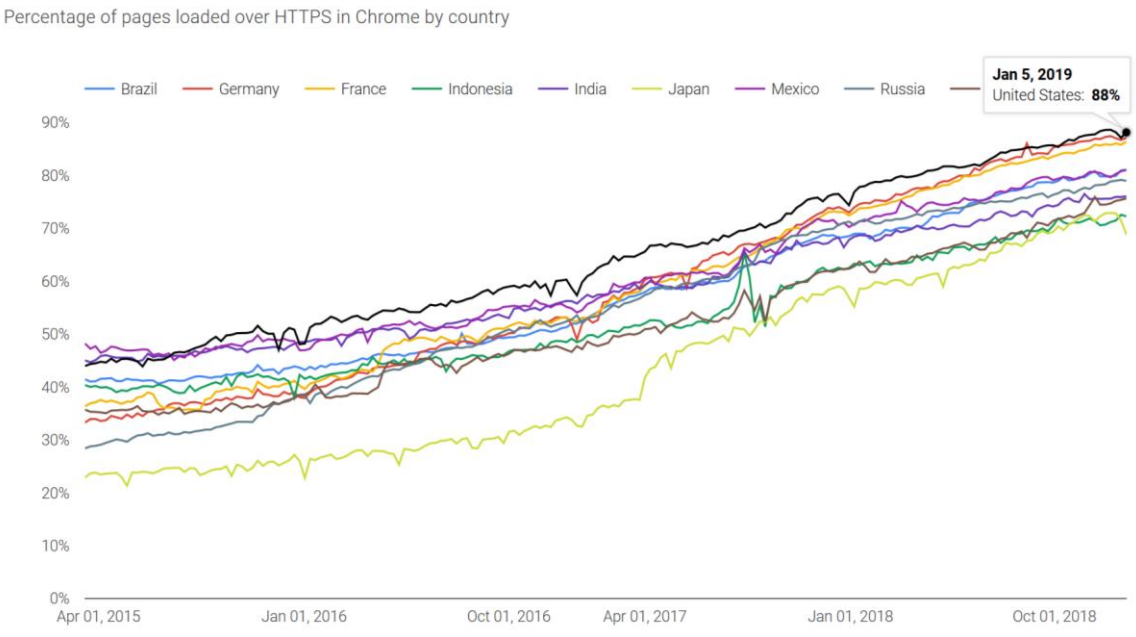
Encrypted traffic growing rapidly due to increased total amount of traffic and % of traffic encrypted



99,202 views | Aug 17, 2013, 08:15am

Forbes

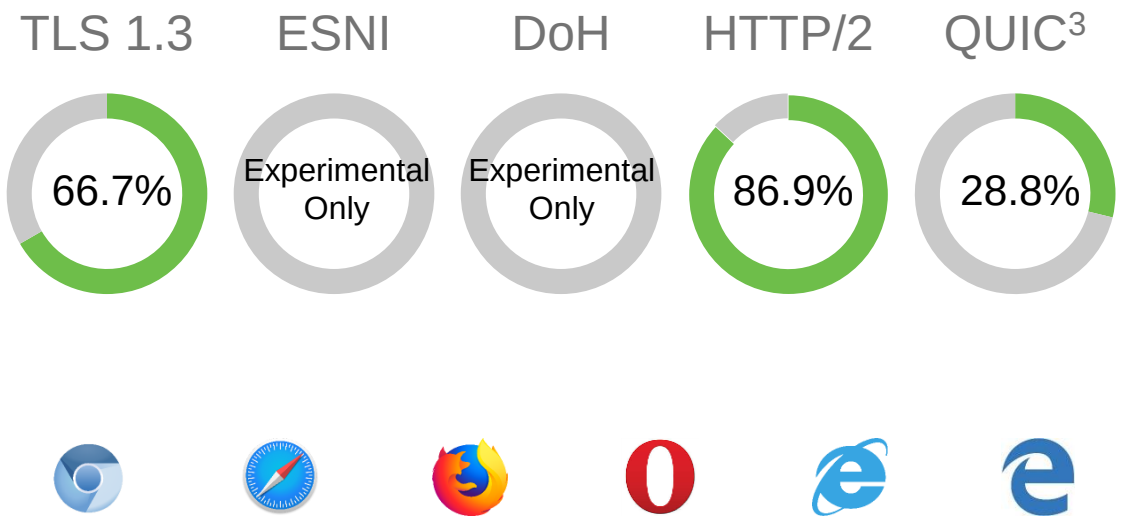
Fascinating Number: Google Is Now 40% Of The Internet



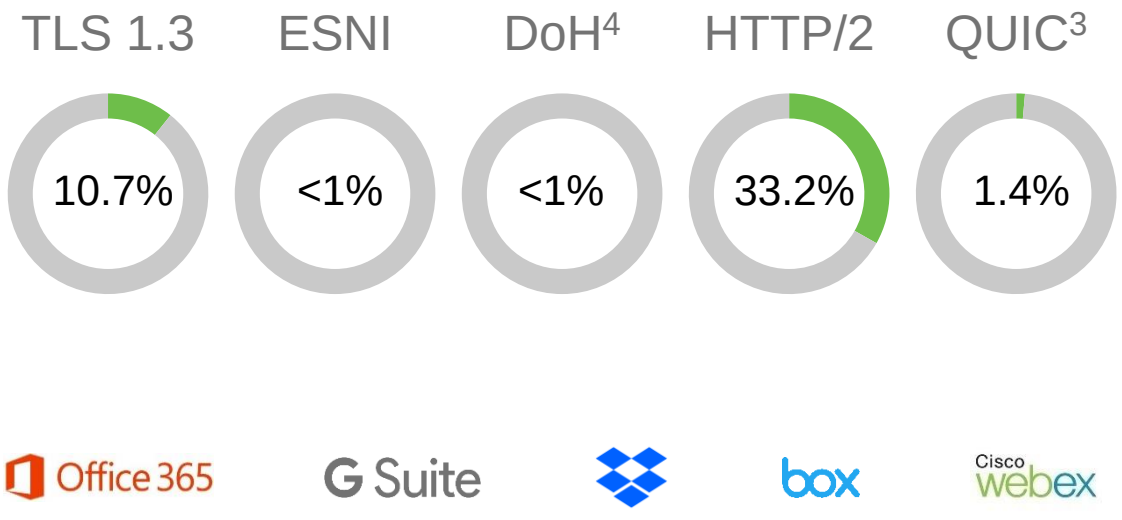
Source: Google Transparency Report, Forbes, Cisco VNI

Browsers and applications investigated

Browser users with the new protocols by default[1]



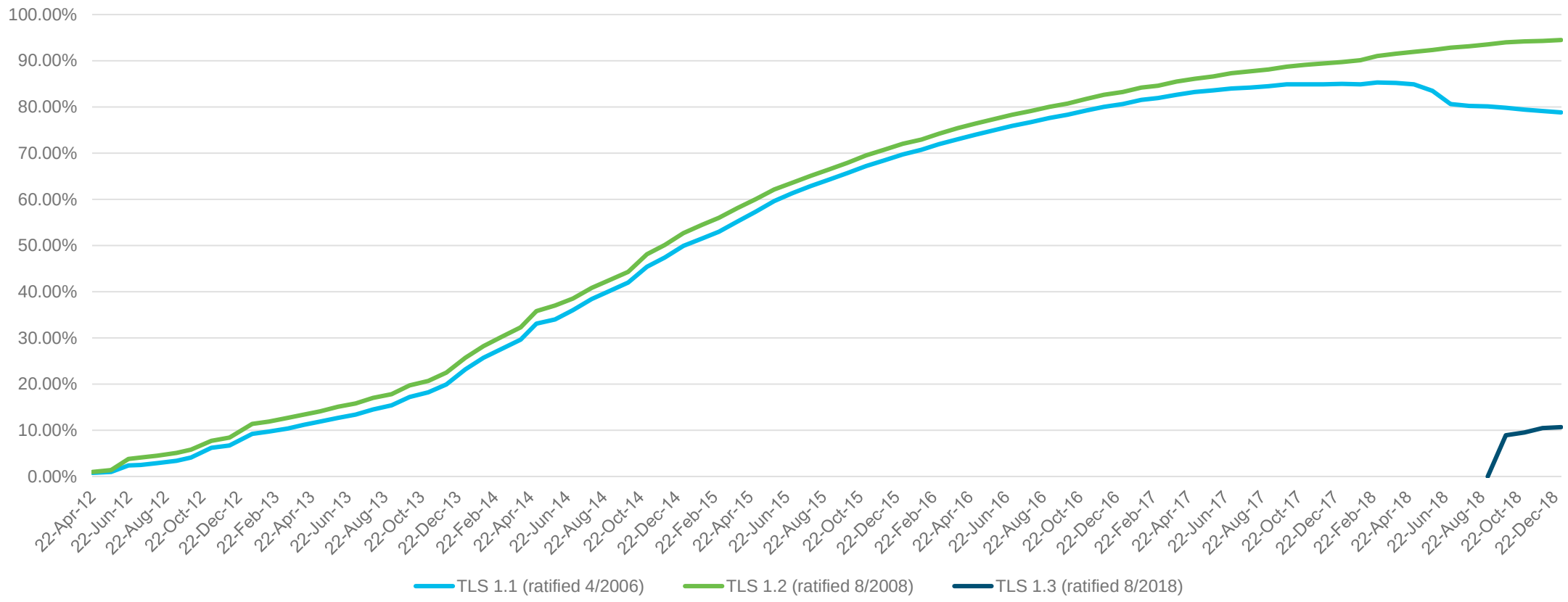
Websites that offer new protocols[2]



Browsers are quickly adopting the emerging standards; many will become the default settings on in next releases. Applications are moving slower, but are beginning to adopt these standards.

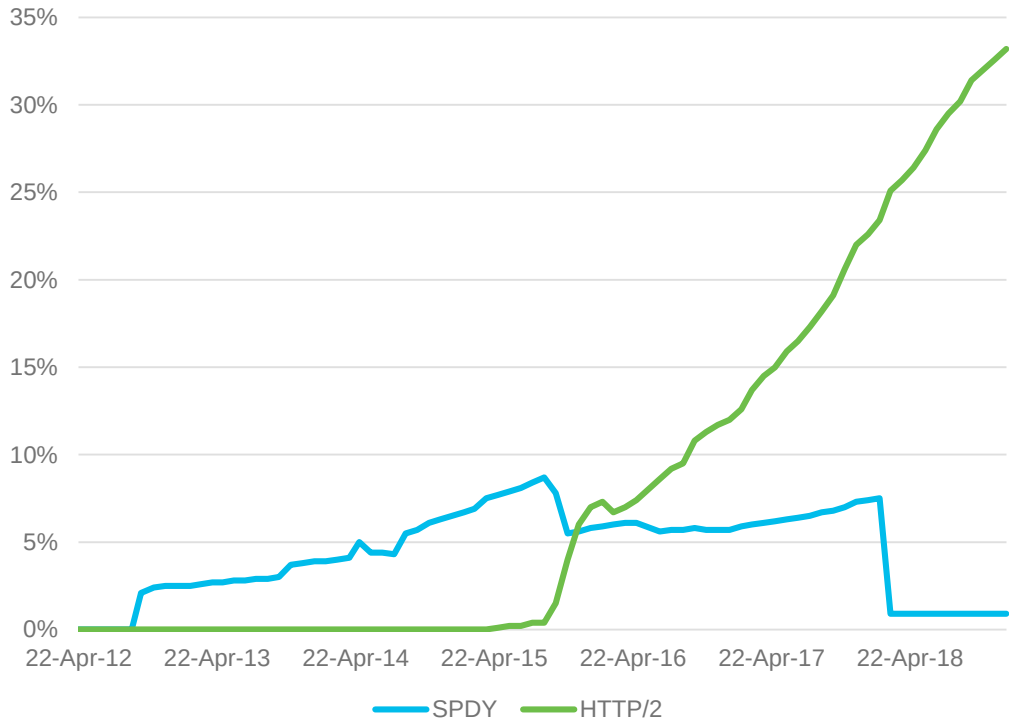
As of January 2019 [1]Based on % of users per browser version that supports standard by default [2]SSL Labs' review of the top 150K sites [3]gQUIC [4]DNS traffic
Source: caniuse.com, Cloudflare blog, Chromium blog, Mozilla blog, ZDNet

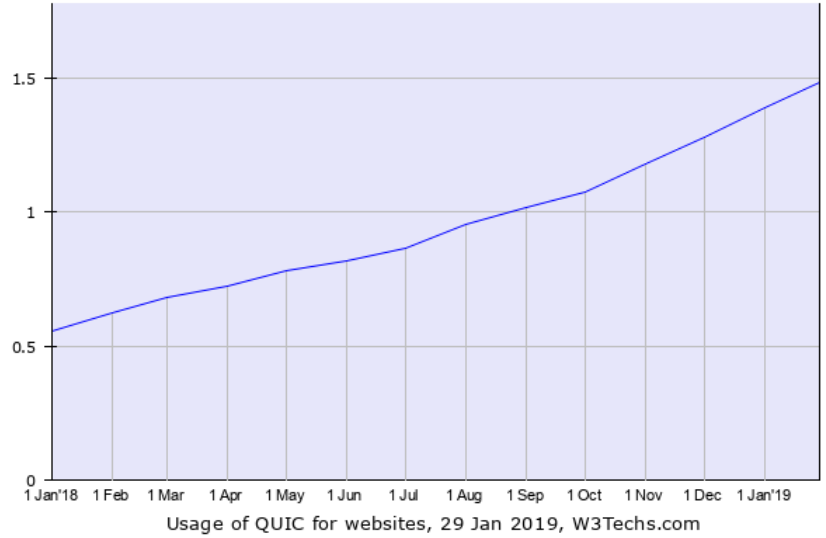
TLS website adoption



Source: SSL Labs

HTTP/2 and HTTP/3 website adoption

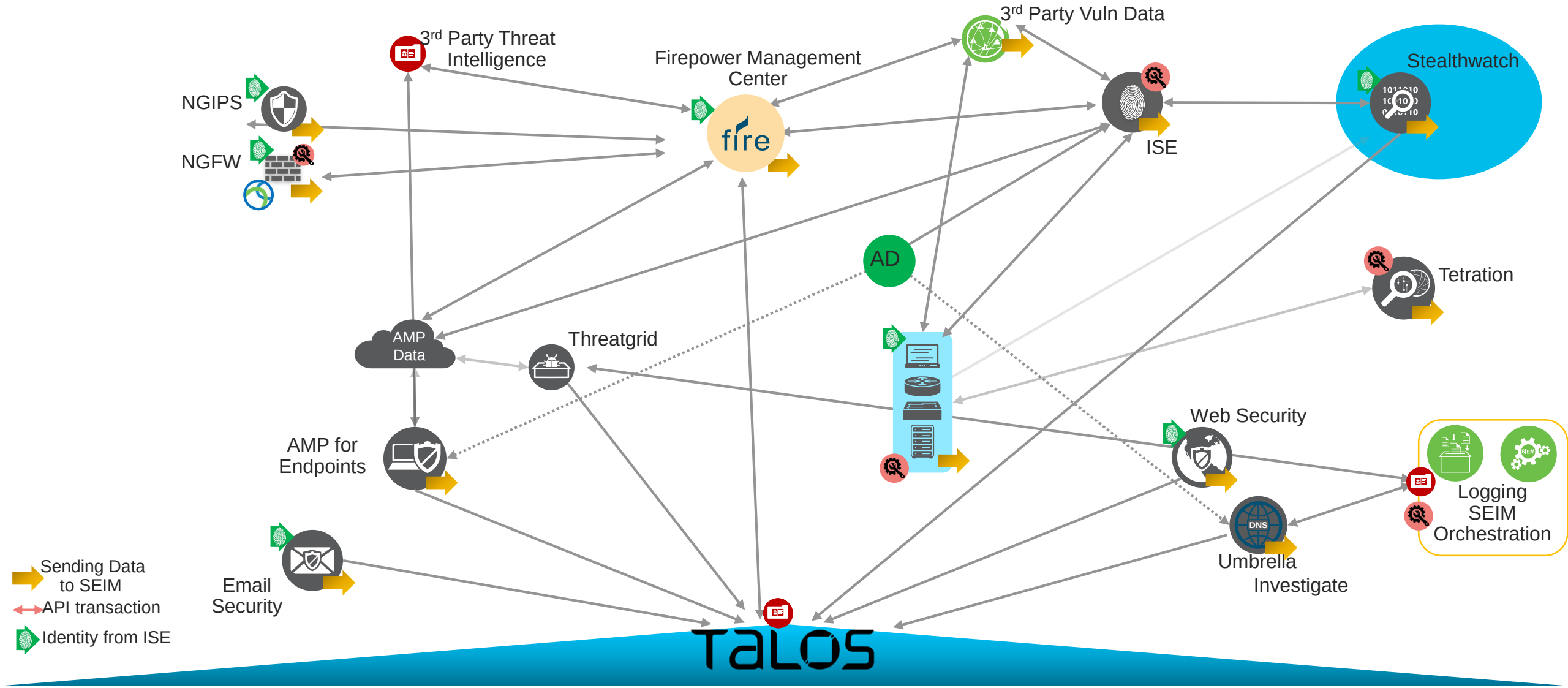




Source: SSL Labs, W3Tech

Architecture in Cyber Security

Security is an Integration Game



Effective security depends on total **visibility**

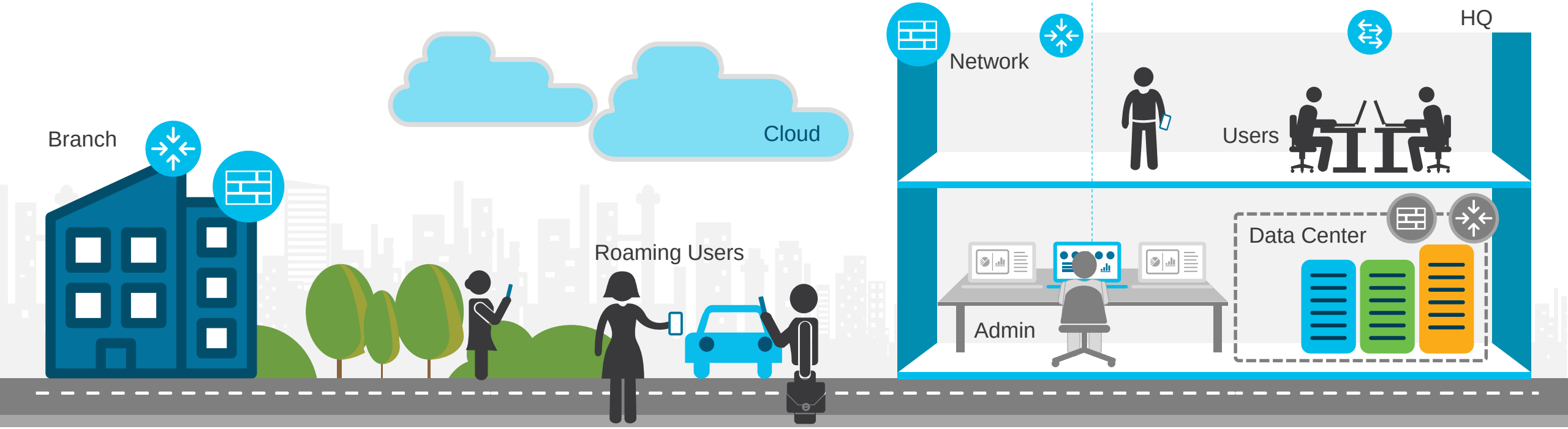
KNOW
every host

SEE
every conversation

Understand what
is **NORMAL**

Be alerted to
CHANGE

Respond to
THREATS quickly

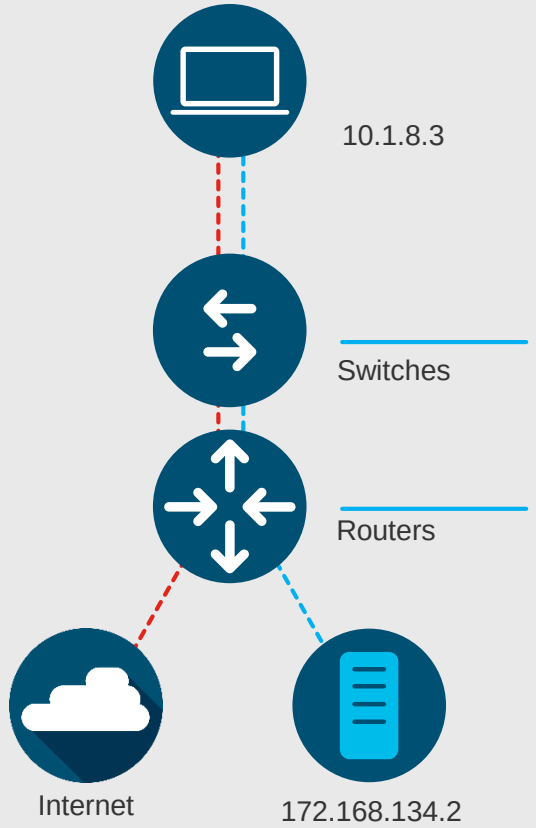


Understand Threat Detection using Flows

The network is a valuable data source

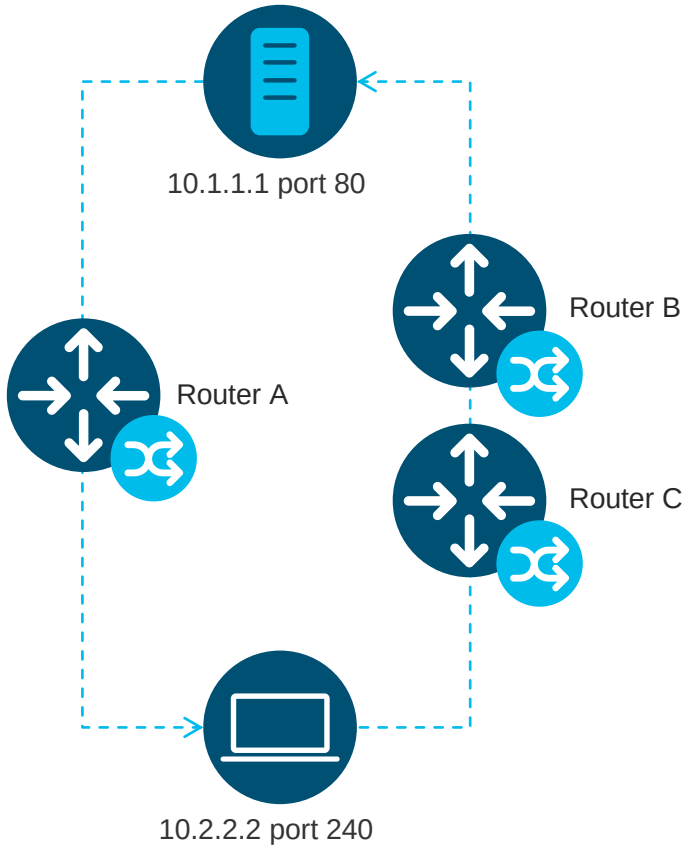
What it provides:

- 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

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

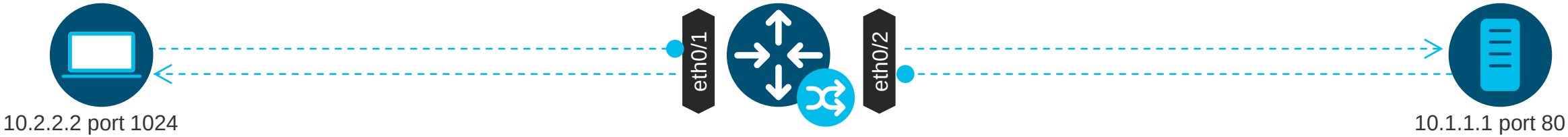
Router C: 10.2.2.2:1024 → 10.1.1.1:80

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

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

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

Stealthwatch Enterprise also enables telemetry ingestion from many third-party exporters

The general ledger

Session Data | 100% network accountability

Client	Server	Translation	Service	User	Application	Traffic	Group	Mac	SGT	Encryption TLS/SSL version
1.1.1.1	2.2.2.2	3.3.3.3	80/tcp	Doug	http	20M	location	00:2b:1f	10	TLS 1.2

Visibility

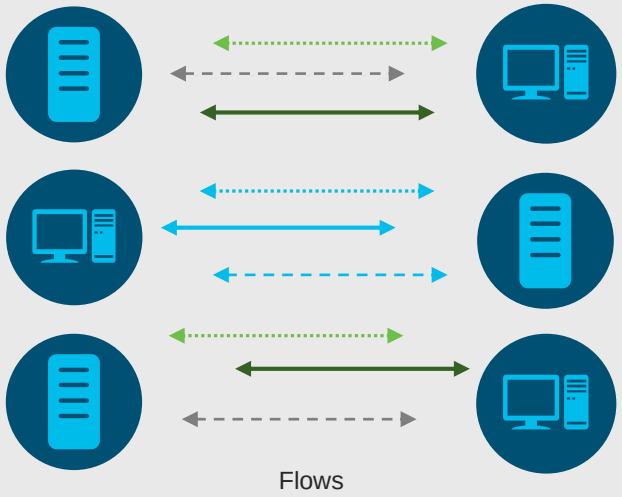
User Information | Network Telemetry | Interface Information | Policy Information | Threat Intelligence | Encrypted Traffic Analytics | Group / Segment | NAT/Proxy | LAYER 7 | Endpoint | Cloud

Security Analytics

Anomaly detection using behavioral modeling

Collect and analyze telemetry

Comprehensive data set optimized to remove redundancies



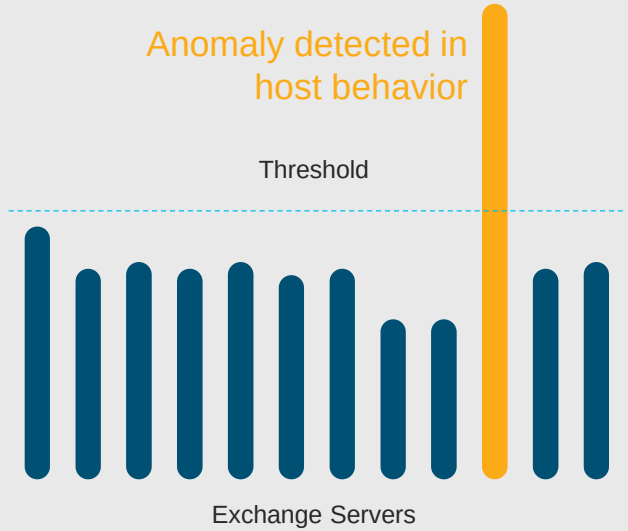
Create a baseline of normal behavior

Security events to detect anomalies and known bad behavior

~100 Security Events		
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

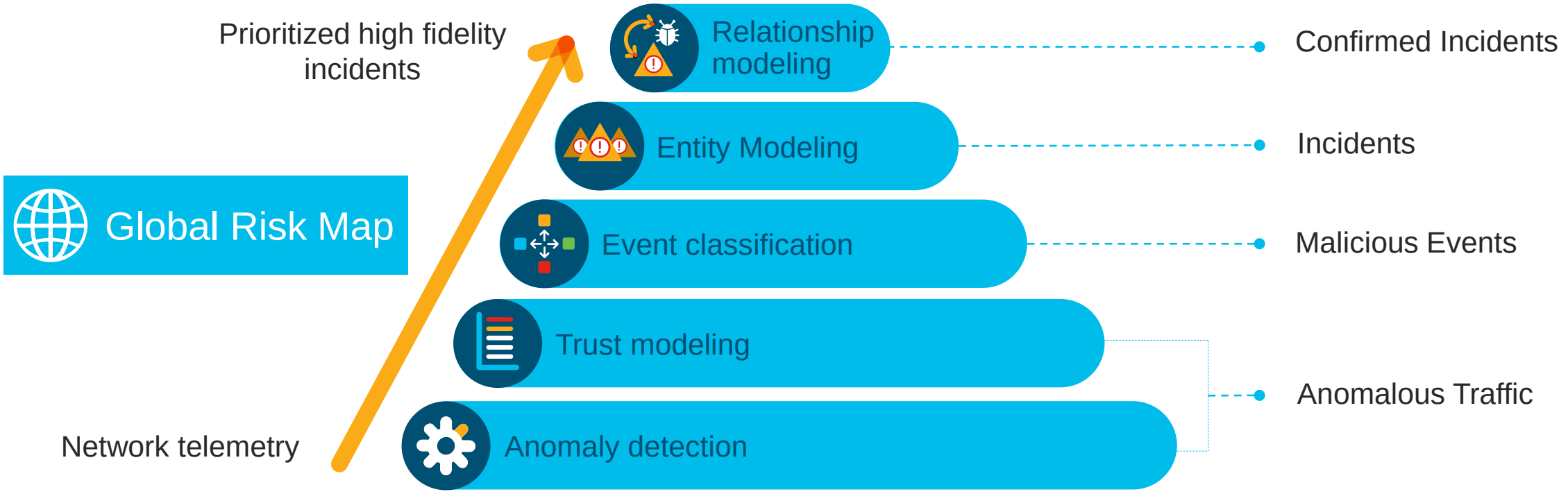
Alarm on anomalies and behavioral changes

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



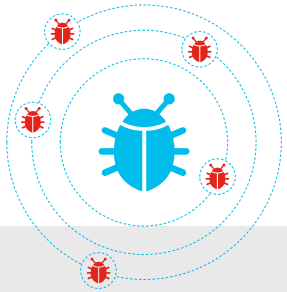
Power of multilayered machine learning

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

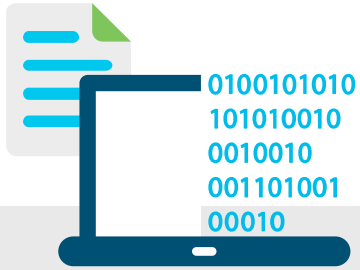


Encrypted Traffic Analytics

Cisco Stealthwatch Enterprise is the only solution providing visibility and malware detection without decryption



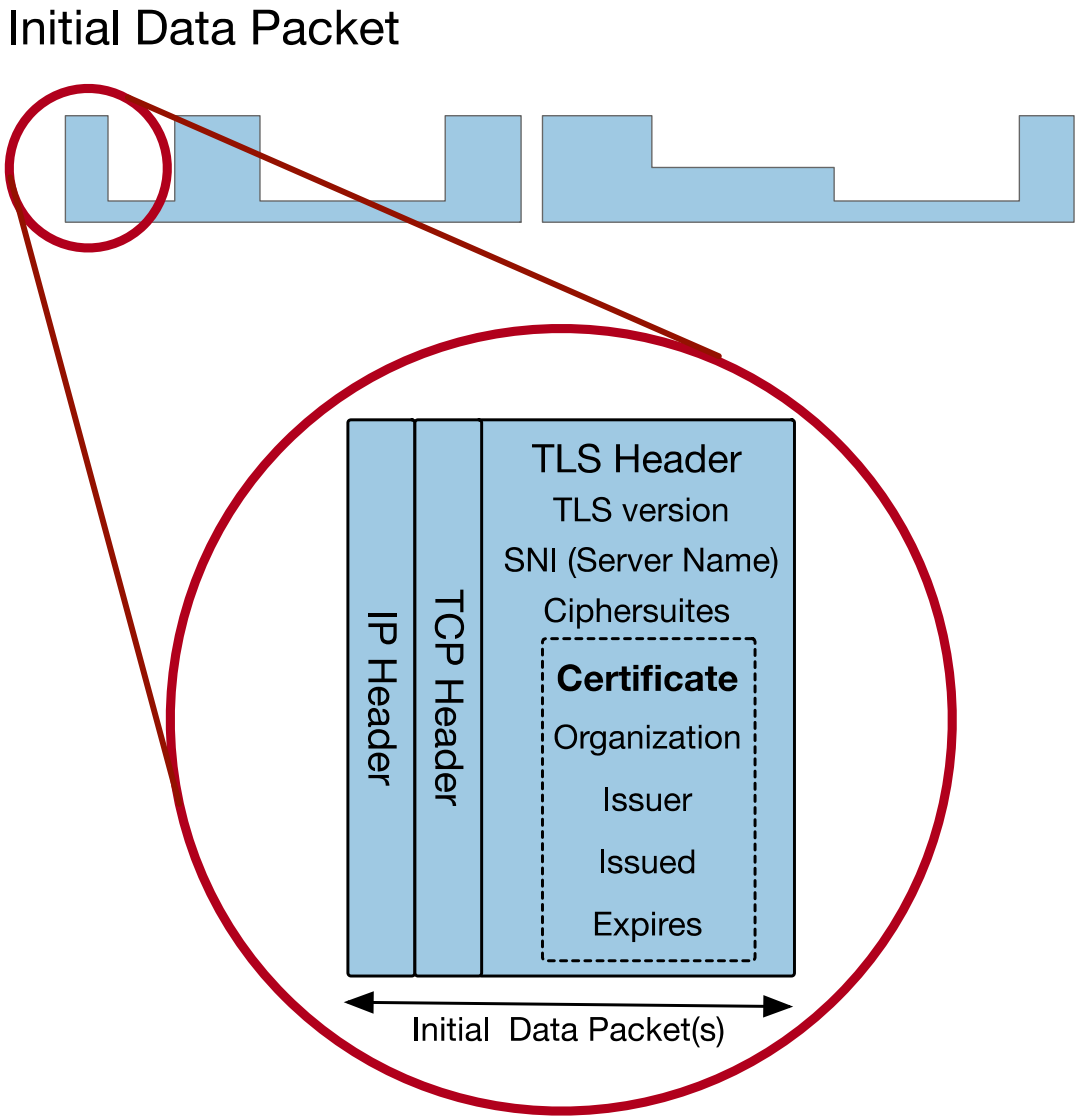
Detect malware
in encrypted traffic



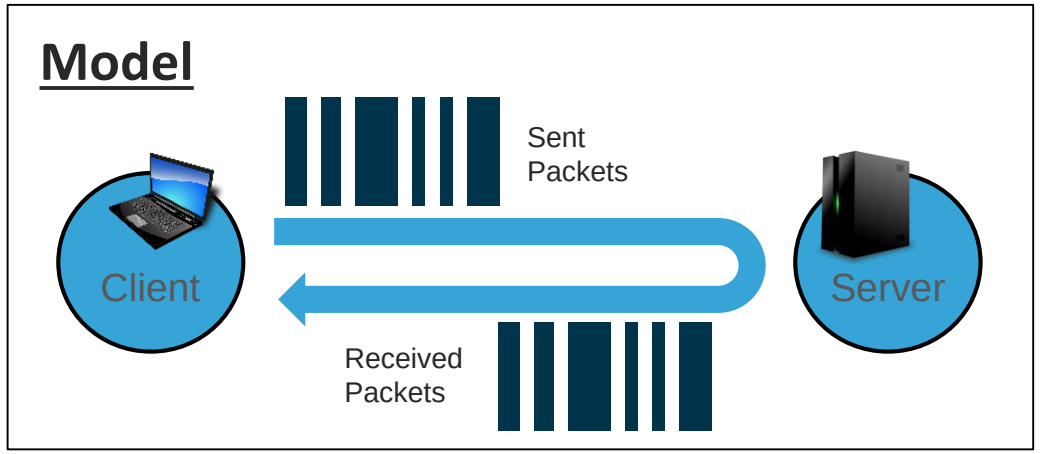
Ensure cryptographic
compliance

Initial Data Packet (IDP)

- HTTPS header contains several information-rich fields
- Server name provides domain information
- Crypto information educates us on client and server behavior and application identity
- Certificate information is similar to *whois* information for a domain
- And much more can be understood when we combine the information with global data



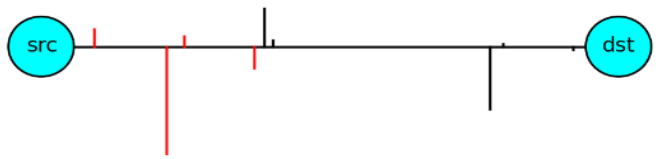
Sequence of Packet Lengths and Times (SPLT)



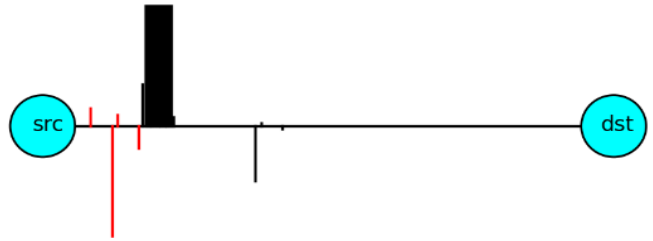
Packet lengths, arrival times and durations tend to be inherently different for malware than benign traffic.

Google search Page Download

Initiate Command & Control



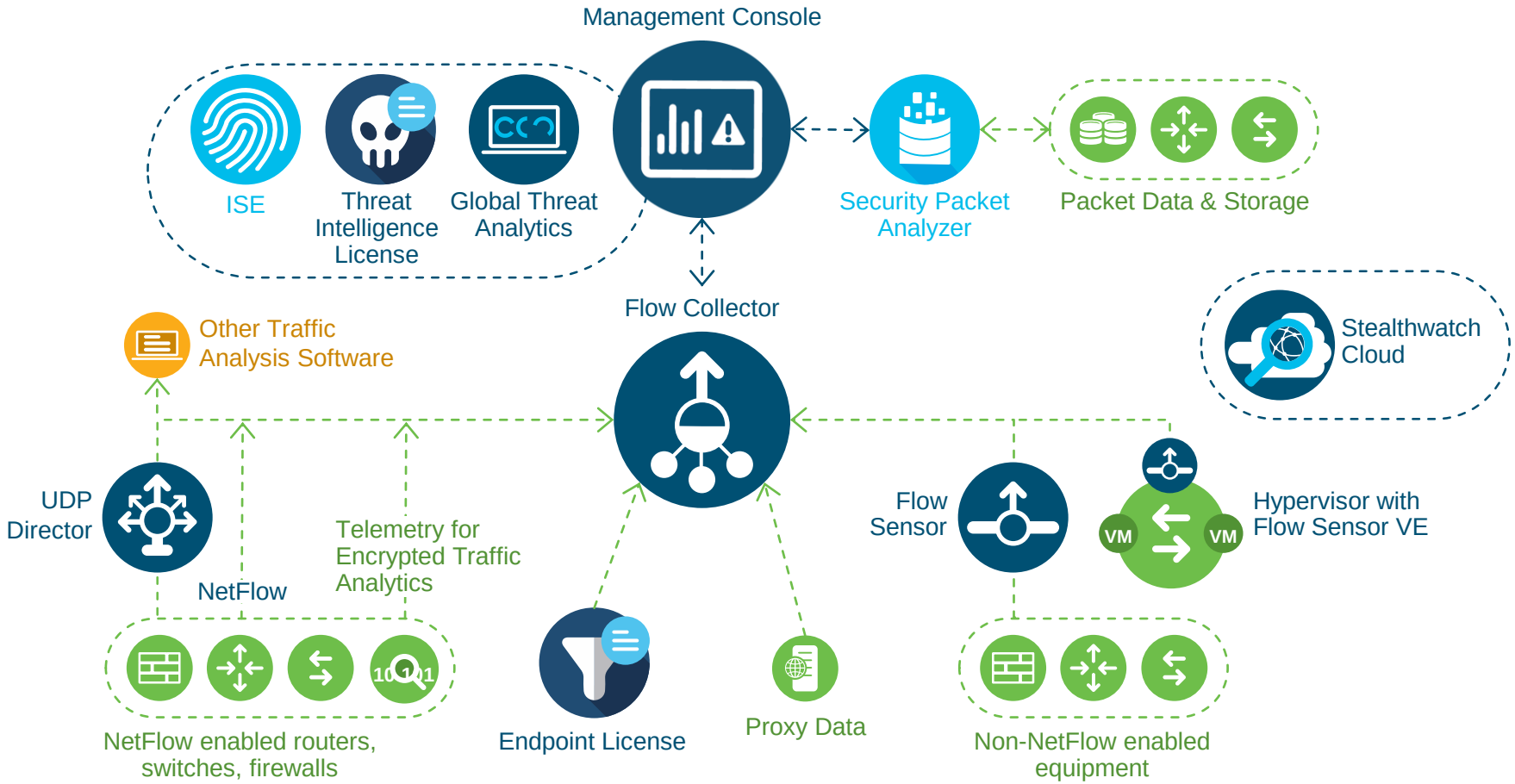
Exfiltration & Keylogging



Deployment

Stealthwatch Enterprise Architecture

Comprehensive visibility and security analytics



Example of Detection

Network Behavior and Anomaly Detection

Alarm Model

- Monitor activity and alarm on suspicious conditions
- Policy and behavioral

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Source User	Details	Last Active
5/29/15 12:00 PM	Atlanta, Sales and Marketing, Desktops	10.201.3.18	--	Multiple Hosts	Suspect Data Hoarding	10.201.3.18	--	Observed 23.9G bytes. Policy maximum allows up to 50M bytes.	5/29/15 1:05 PM
5/29/15 11:20 AM	Terminal Server, Datacenter	10.201.0.23	--	Multiple Hosts	Suspect Data Hoarding	10.201.0.23	--	Observed 38.45G bytes. Policy maximum allows up to 50M bytes.	5/29/15 2:40 PM

Scoped Worm activity

Manage Columns | Export

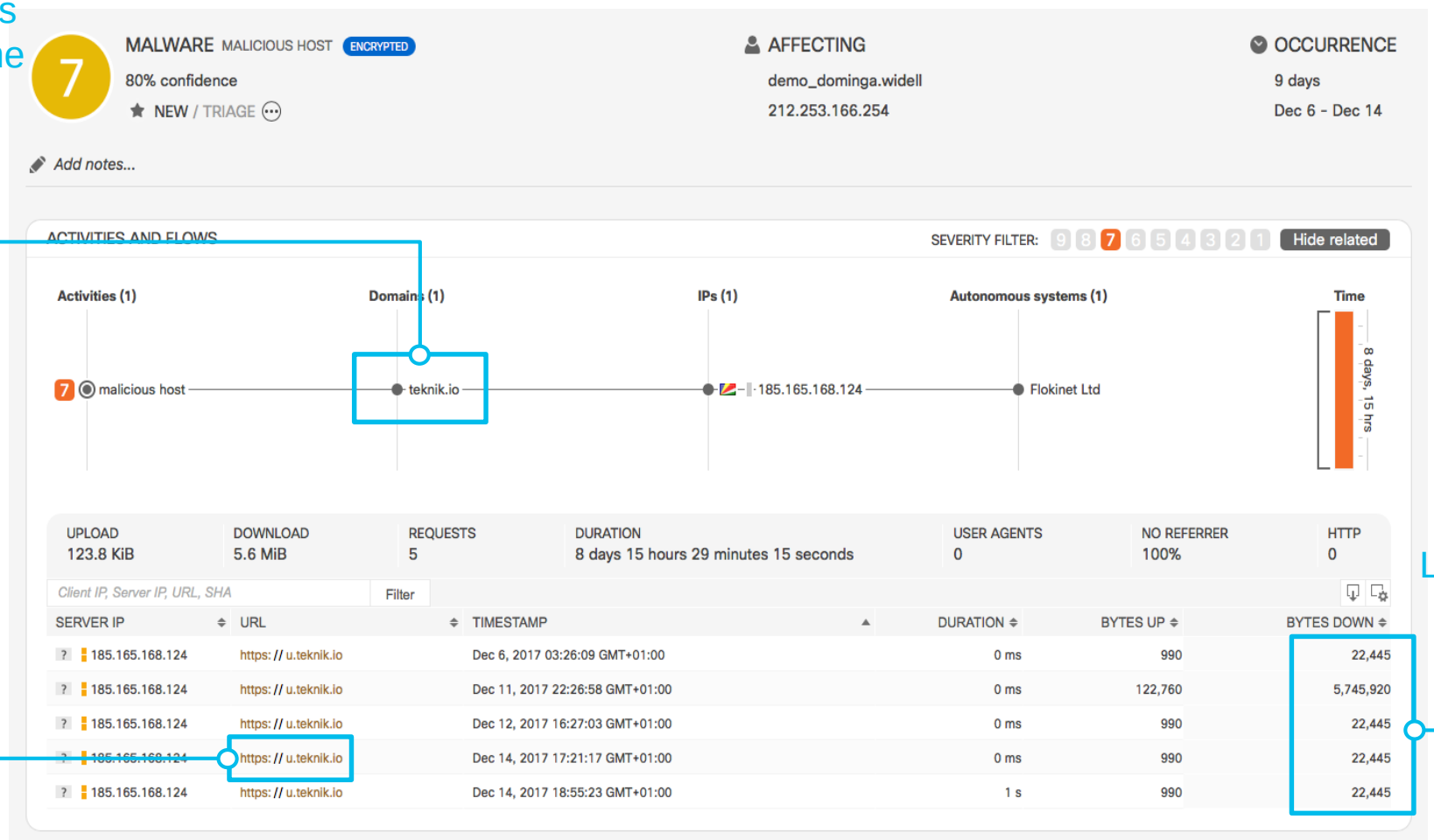
% OF BYTES	HOST IP ADDR...	HOST NAME	HOST GROUPS	HOST ROLE	BYTES	PACKETS	FLOWS	PEERS	HOST BYTES R...
19.49%	10.201.3.83	--	End User Devices , Desktops , Atlanta , Sales and Marketing	Client	4.35 M	13.26 K	12,387	4,860	92.63%
11.42%	10.201.3.50	workstation-050	End User Devices , Desktops , Atlanta , Sales and Marketing	Client	2.55 M	8.68 K	8,177	3,580	92.81%

Found 15 scanning systems

Scoped the investigation systems

Example Detection: Malware with encrypted C&C

Passive DNS attribution & Global Risk Map tracks servers likely to become part of an attack

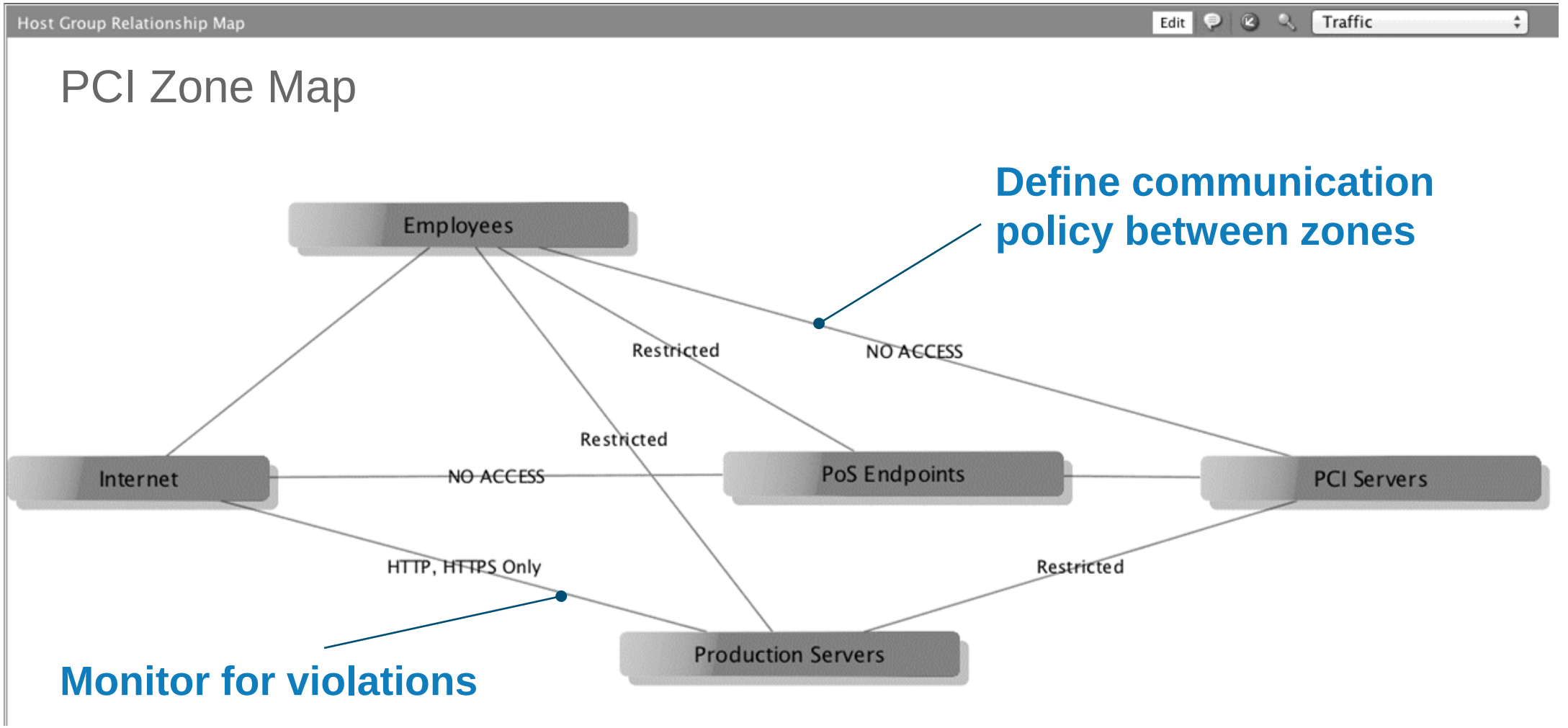


Original URL request extracted from the new ETA telemetry (IDP)

Sequence of Packet Lengths and Times (SPL

Policy Violation Detection

Segmentation Monitoring with StealthWatch



Modeling Policy: Alarm Occurrence

Alarm dashboard showing all policy alarms

demo.local | Alarm Dashboard : Policy Violation (1)

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Policy	Event Alarms	Source User	Details
5/25/15 4:42 PM	Catch All	10.10.18.102	--	Multiple Hosts	Inside Hosts	Employee to Production Servers	employee1	Expected 1 points, tolerance of 75 allows up to 300k points.

Details of "Employee to Production Servers" alarm occurrences

demo.local | Alarms : Employee to Production Servers for 5/25/2015 (1)

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Source User	Details	Last Active	Active	Acknowledged
5/25/15 4:42 PM	Catch All	10.10.18.102	Catch All	10.3.200.10	Employee to Production Servers	Inside Hosts	employee1	View Details	Current	Yes	No

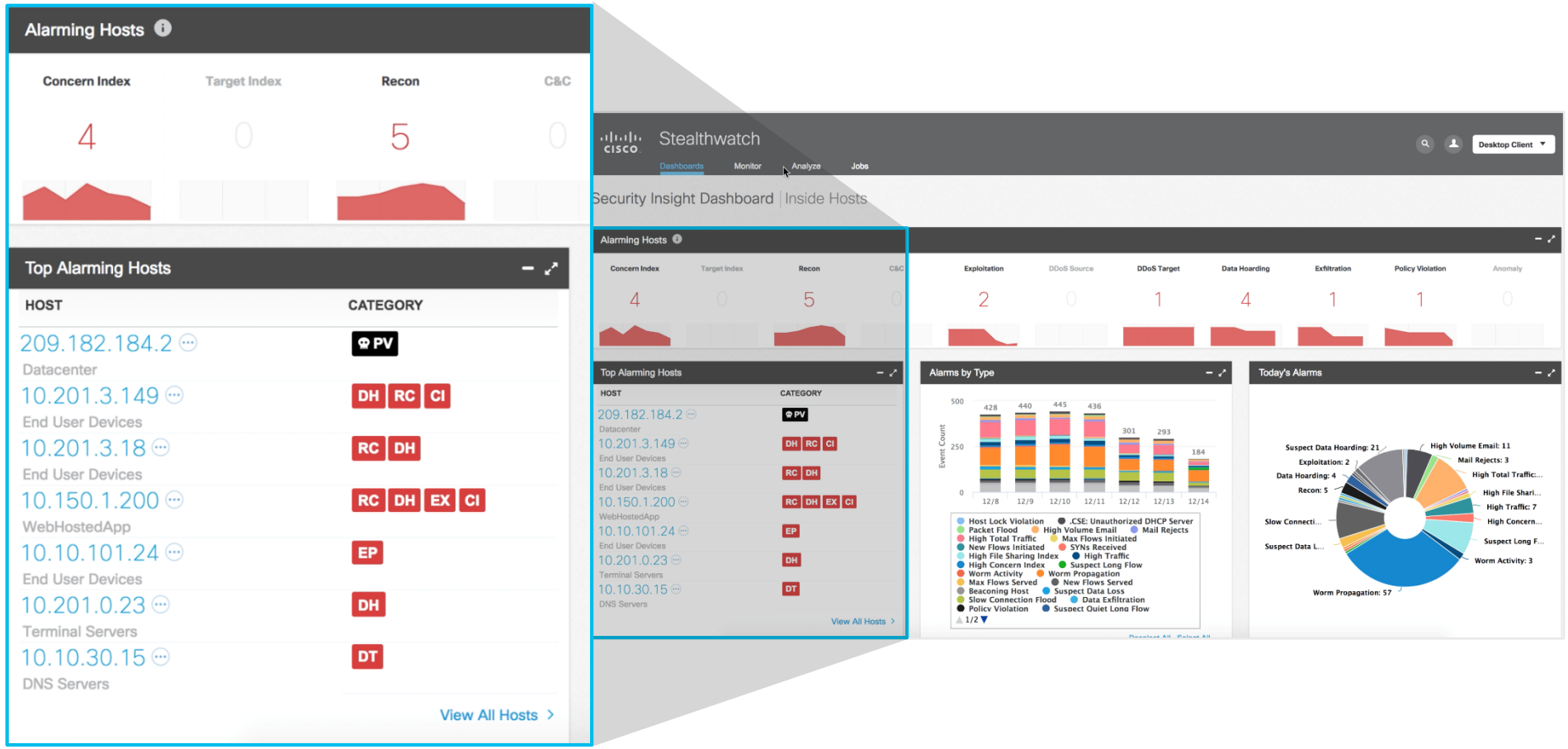
From Visibility to Rapid Threat Containement

Alarms tied to specific entities

Quick snapshot of malicious activity

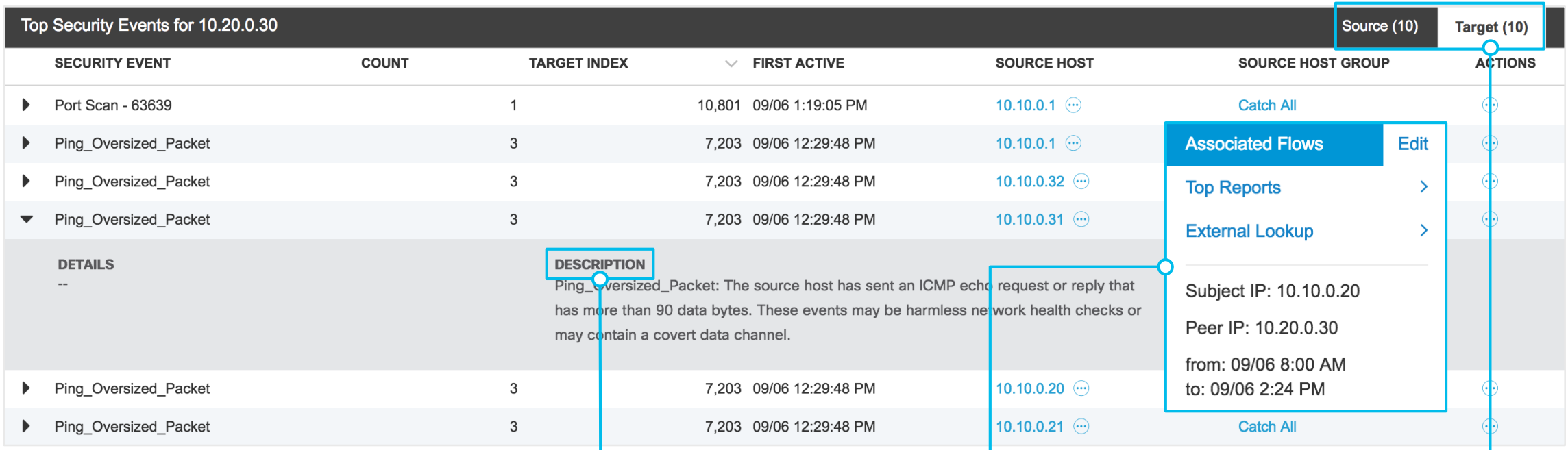
Suspicious behavior linked to logical alarms

Risks prioritized to take immediate action



Investigating a host

Top security events

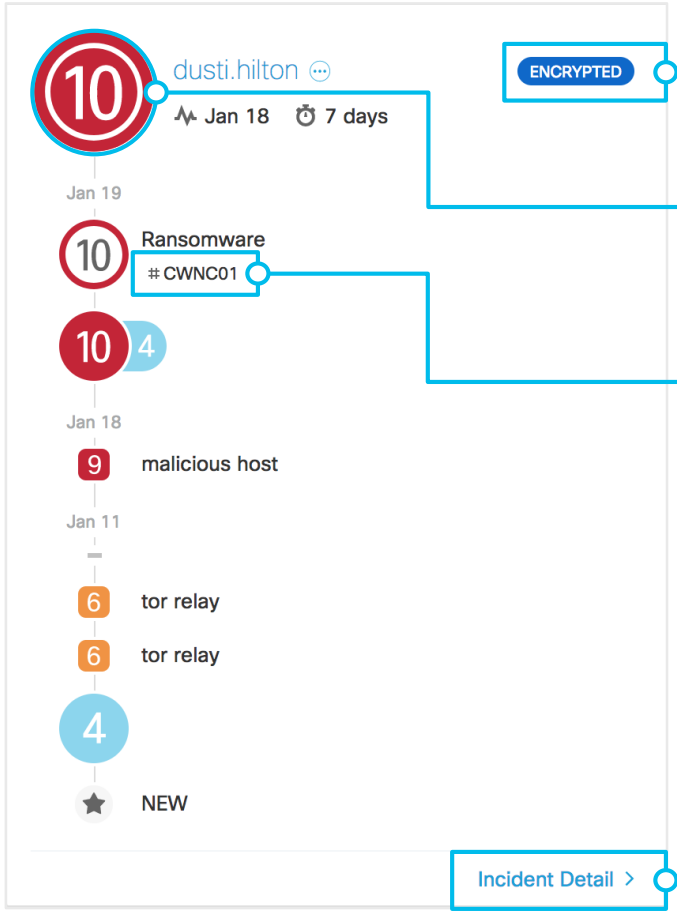


Understand why the alarm was triggered

Drill down into associated telemetry with just one click

Easily determine if the host is the source or target of an attack

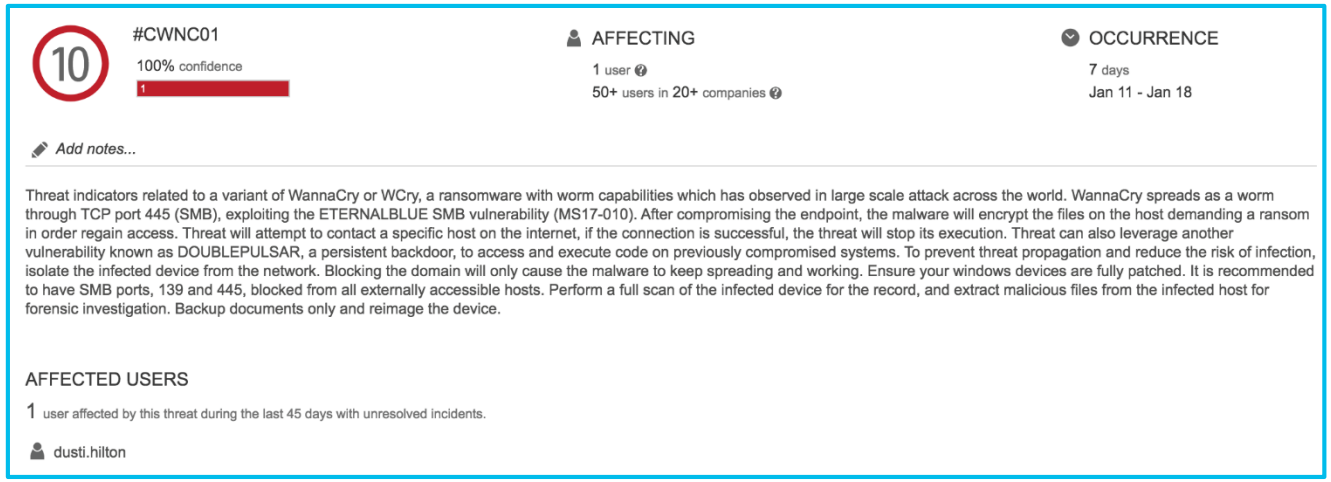
Apply machine learning to investigate threats



Malware behavior detected in encrypted traffic

Threats ranked by overall severity to environment

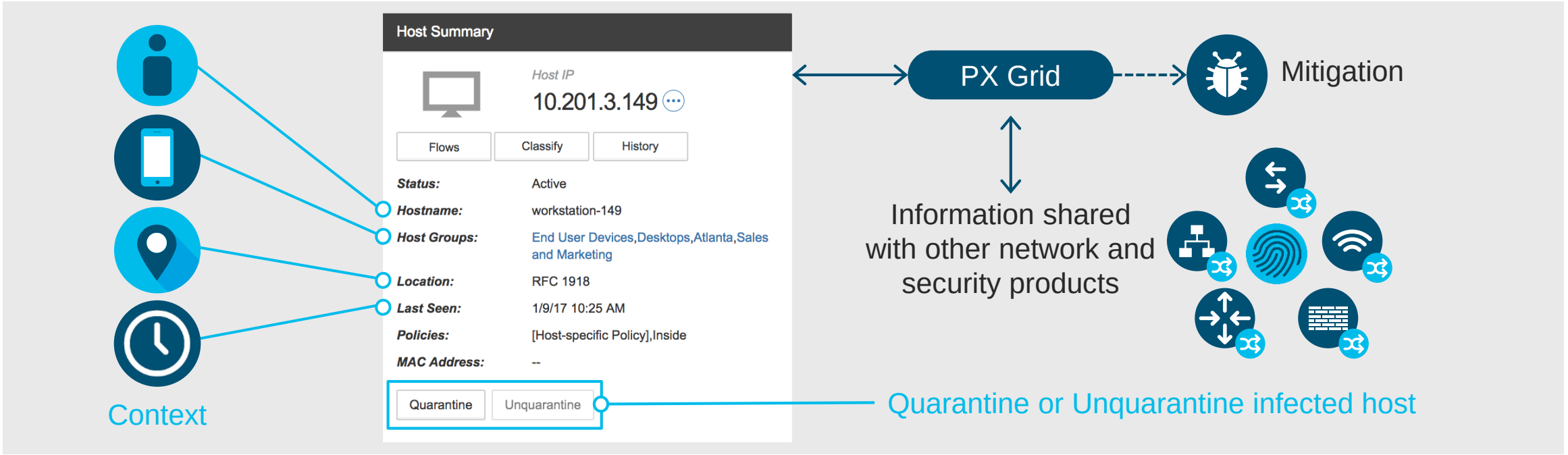
Correlation of global threat behaviors

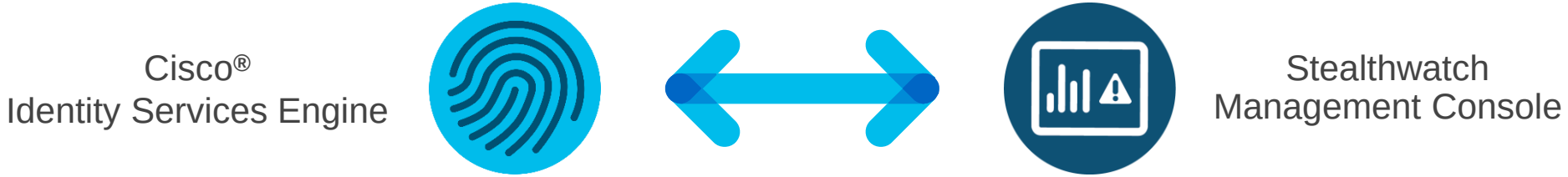


Threat propagation details

Rapid Threat Containment

Without any business disruption





Closing

Security Analytics with Stealthwatch Enterprise

Global threat intelligence

(powered by Talos)

Intelligence of global threat campaigns mapped to local alarms for faster mitigation

Multilayered machine learning

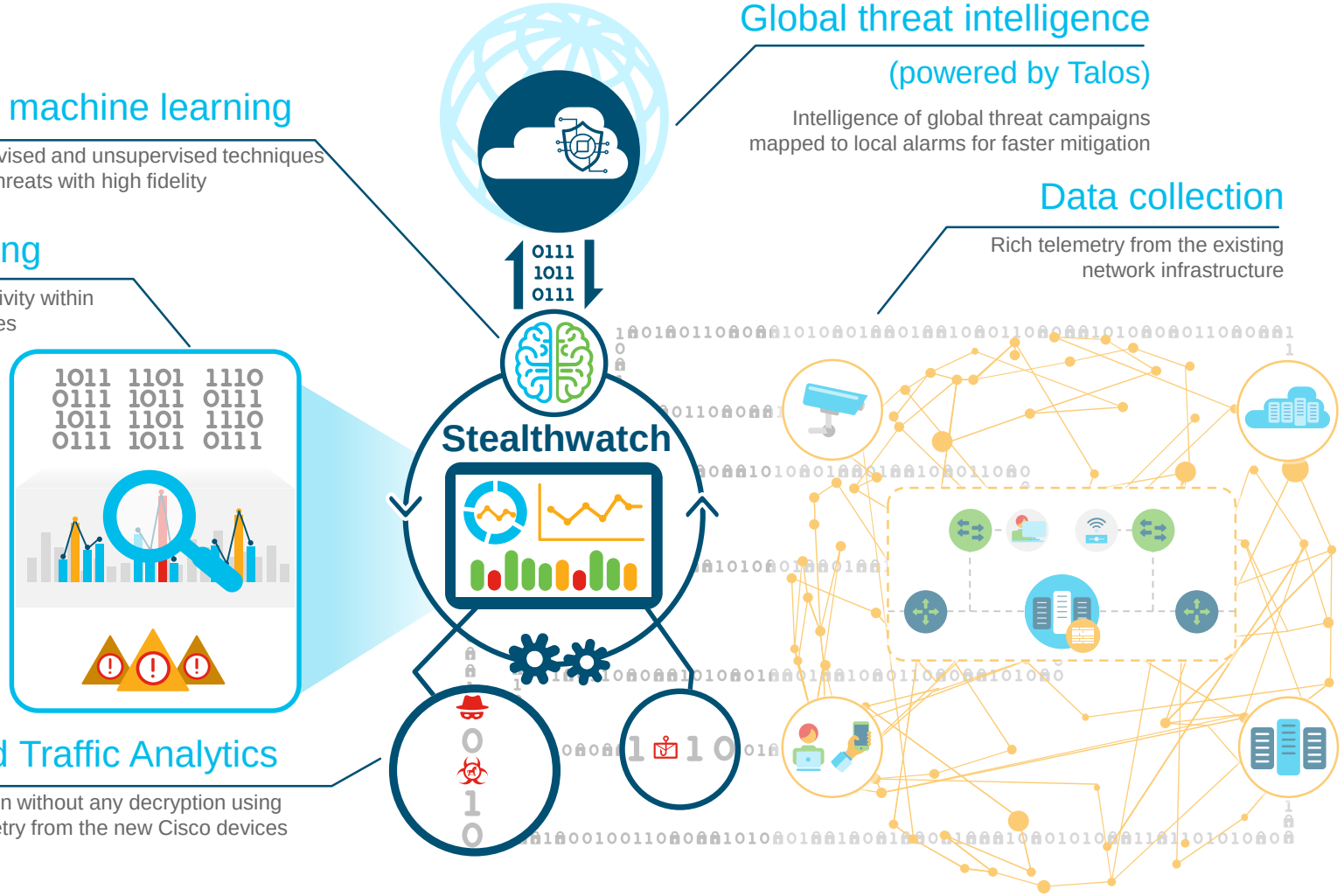
Combination of supervised and unsupervised techniques to convict advanced threats with high fidelity

Behavioral modeling

Behavioral analysis of every activity within the network to pinpoint anomalies

Data collection

Rich telemetry from the existing network infrastructure



Encrypted Traffic Analytics

Malware detection without any decryption using enhanced telemetry from the new Cisco devices


CISCO