Stealthwatch

Kerry Armistead
Director of Product Management

Agenda

- Threat Landscape
- Stealthwatch
- Encrypted Traffic Analytics
- Stealthwatch Cloud
- Cisco Stealthwatch Online Visibility Assessment

Digital business has expanded the attack surface

Enterprise Mobility

Cloud

21B

By 2020, IoT devices that will access the network

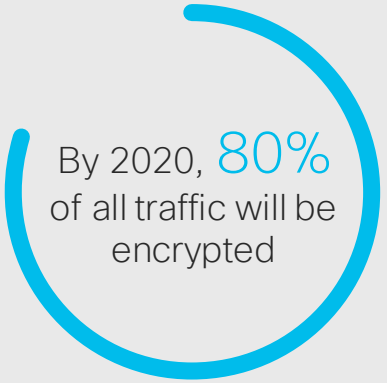
Encrypted Traffic

2/3

By 2020, traffic from wireless and mobile devices that will account for total IP traffic

Acquisitions & Partnerships

Internet of Things



Network threats are getting smarter

Motivated and targeted adversaries

State sponsored

Financial/espionage motives

$1T cybercrime market

Insider Threats

Compromised credentials

Disgruntled employees

Admin/privileged accounts

Increased attack sophistication

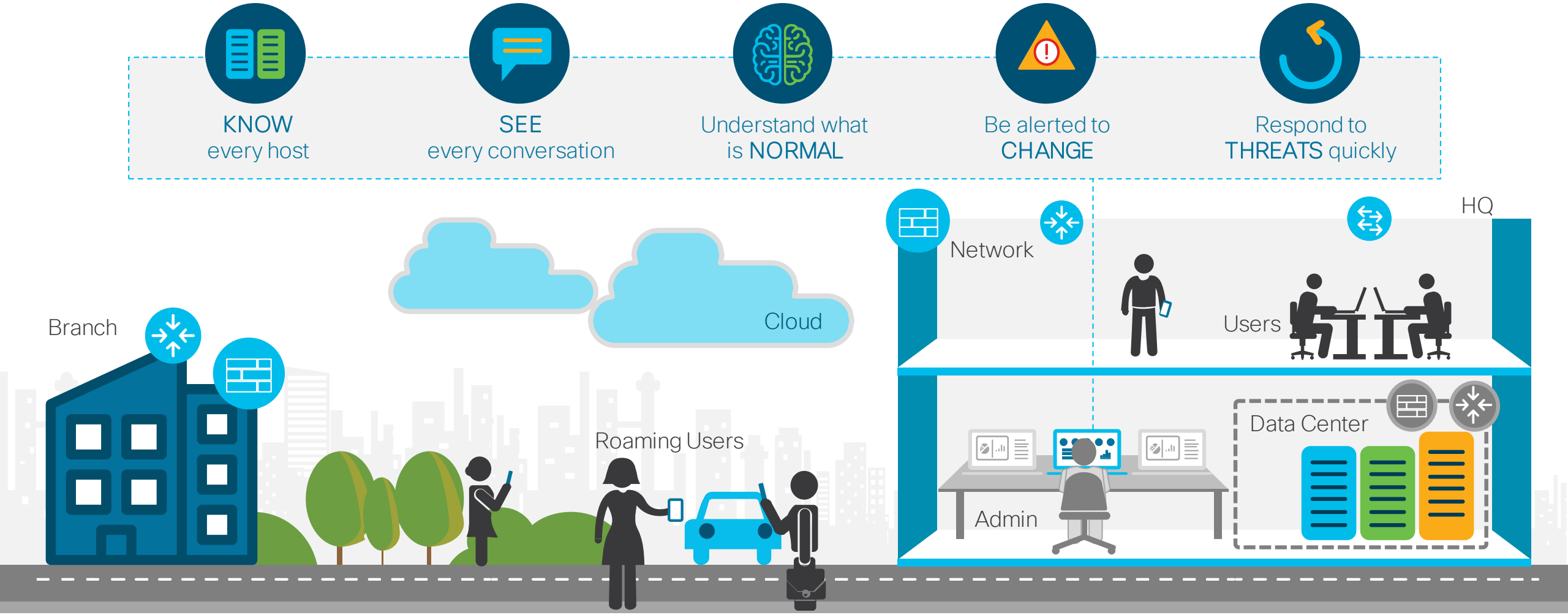
Advanced persistent threats

Encrypted malware

Zero-day exploits

191 DAYS Industry average detection time for a breach → **66 DAYS** Industry average time to contain a breach → **$3.62M** Average cost of a data breach

Effective security depends on total visibility



Cisco Stealthwatch:
Scalable visibility and security analytics

Most comprehensive visibility for effective security outcomes

Advanced Threat Detection

Accelerated Threat Response

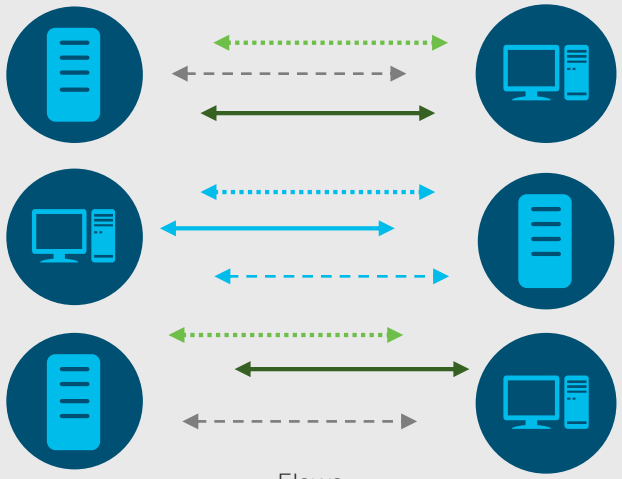
Simplified Network Segmentation

Using existing network infrastructure

Industry-leading Security Analytics

Behavioral and anomaly detection

Collect and analyze telemetry

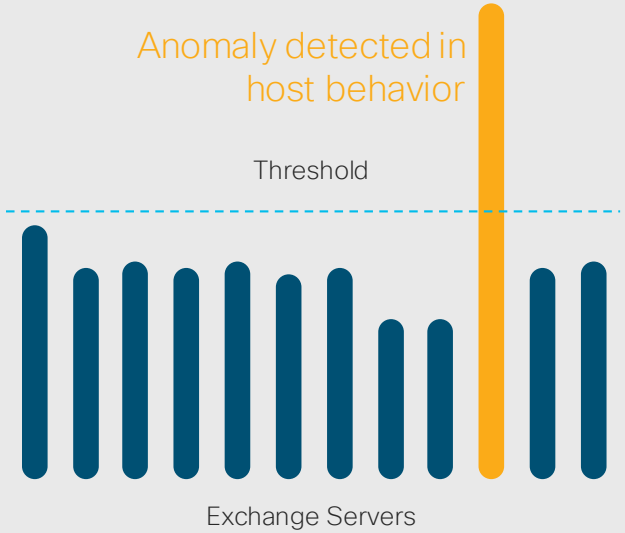


Create a baseline of normal behavior

~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

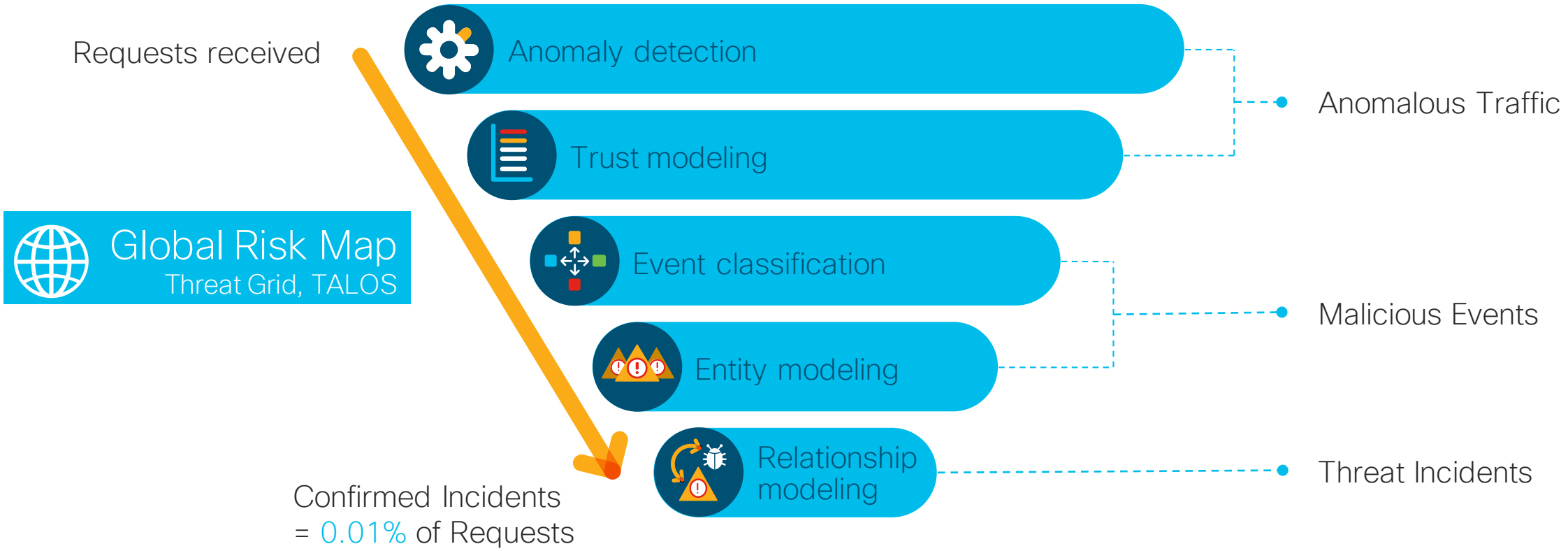
Approximate time required to complete baseline

Alarm on anomalies and behavioral changes



Power of multi-layer machine learning

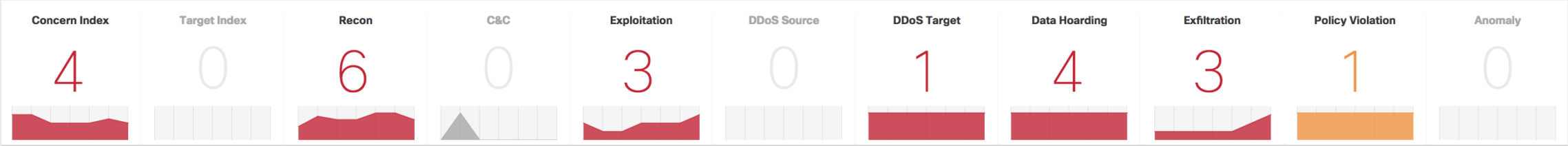
Increase fidelity of detection using best-in-class security analytics



Advanced Threat Detection

Logical alarms based on suspicious events

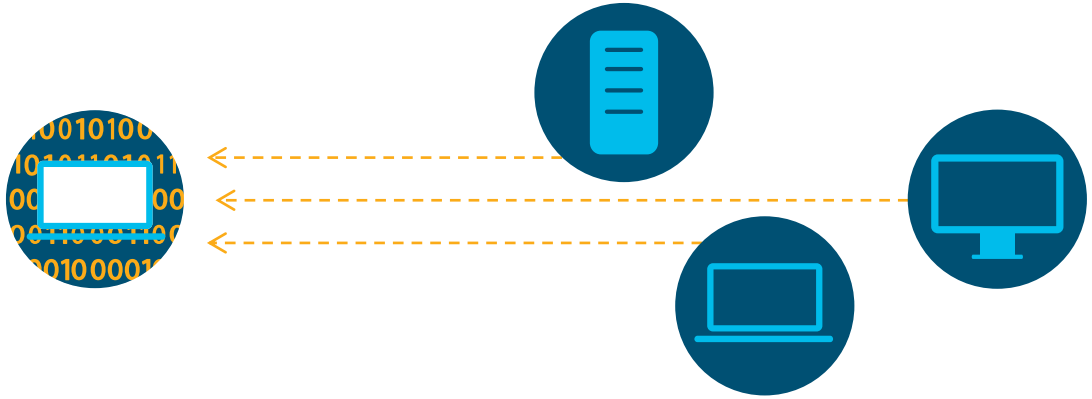
Source or target of malicious behavior	Reconnaissance	Command and Control	DDoS Activity	Insider threats
Scanning, excessive network activity such as file copying or transfer, policy violation, etc.	Port scanning for vulnerabilities or running services	Communication back to an external remote controlling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



Insider threat example: data hoarding

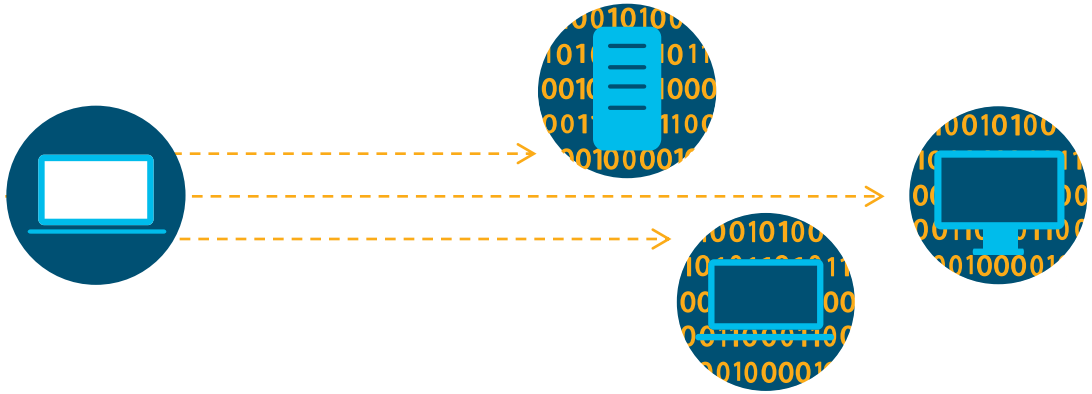
Suspect Data Hoarding

Unusually large amount of data inbound from other hosts



Target Data Hoarding

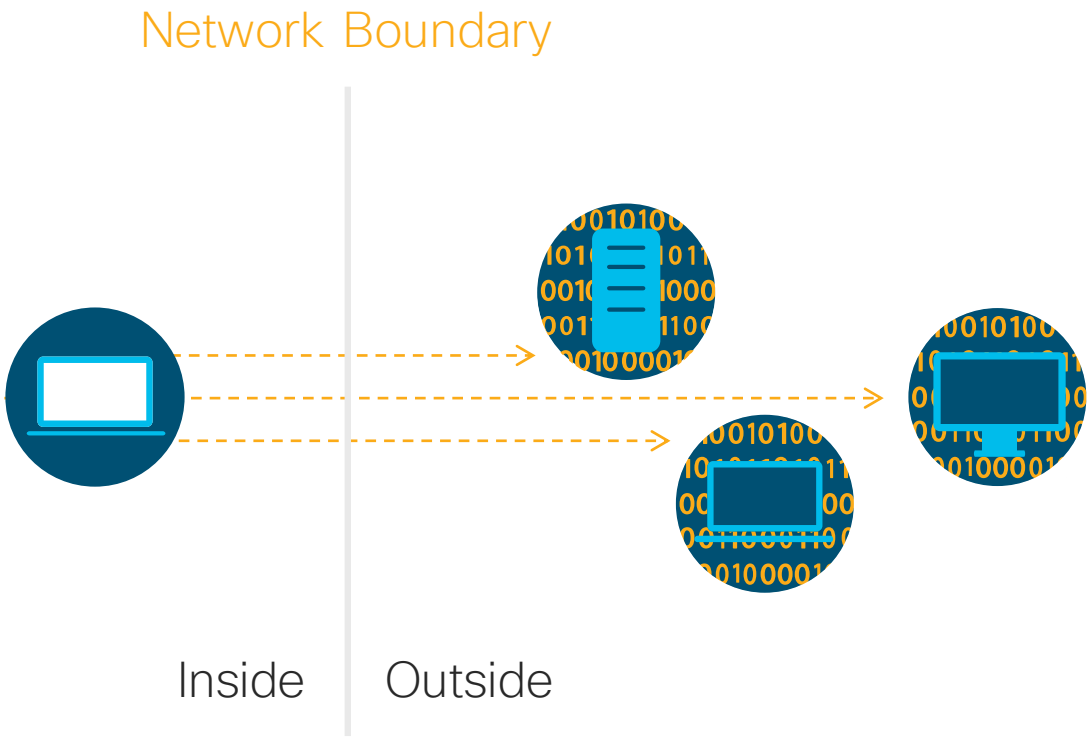
Unusually large amount of data outbound from a host to multiple hosts



Insider threat example: data exfiltration

Data Exfiltration

Unusually large amount of data outbound from a host to one or more external hosts



Accelerated Threat Response

Pinpoint the source of the threat through visibility into each host

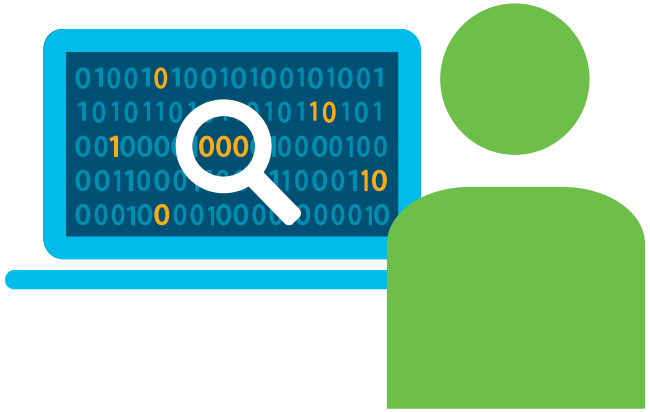
Conduct forensic investigations into past events by analyzing the network audit trails

Mitigate threats easily without business shutdown by using the network

Investigate threats quickly

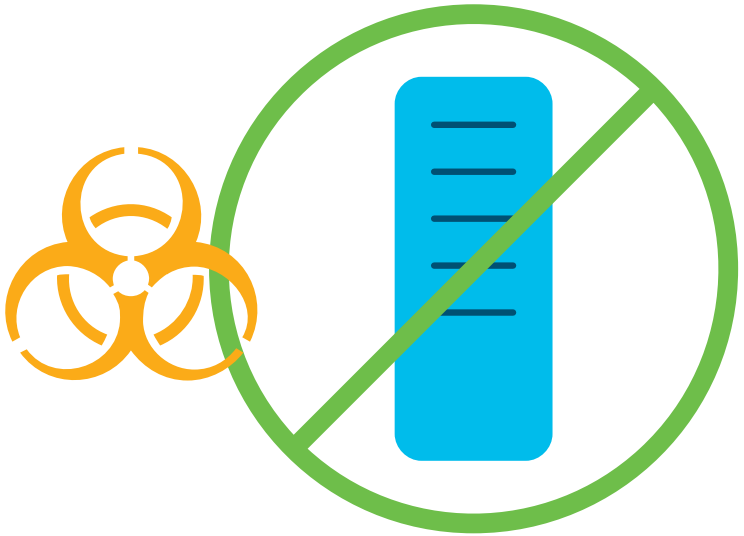
Investigation | Mitigation

- Contextual user and application info
- Top security alarms by hosts
- Drill-down into telemetry associated with security events
- Malware propagation through infected hosts
- Network audit trails for deeper forensics on past/long-running events



Mitigate threats effectively

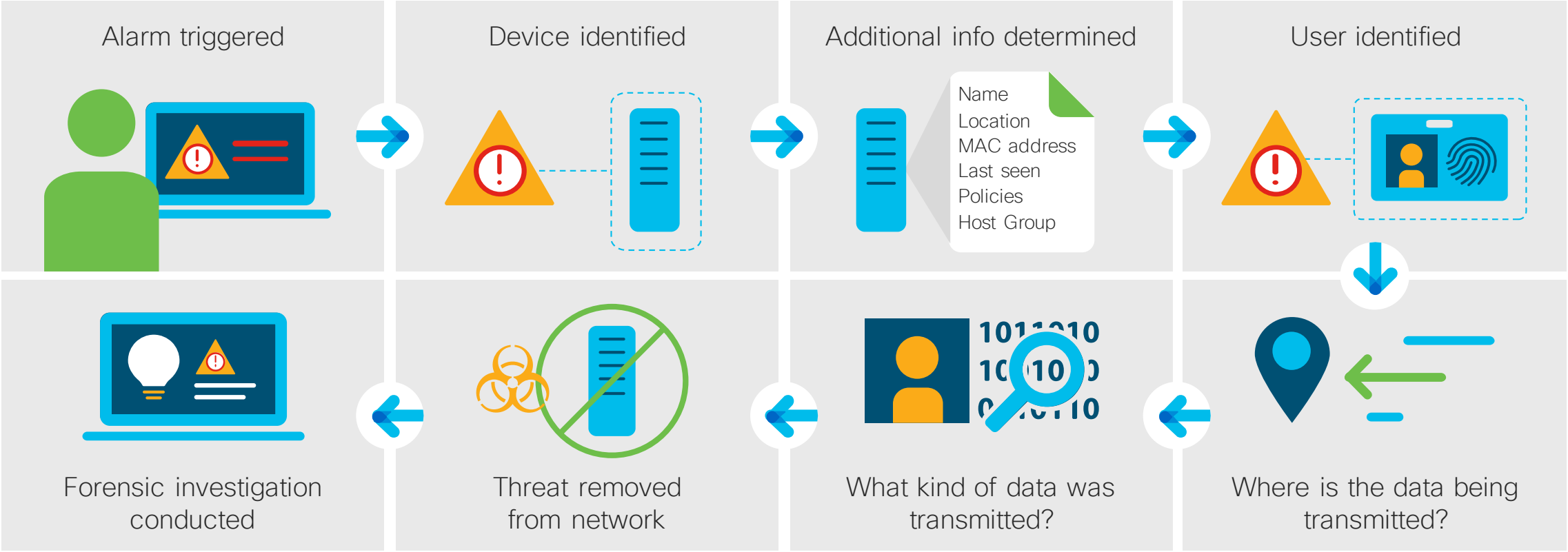
Investigation | **Mitigation**



- An alarm can have an associated response
  - Notify in the alarm table
  - Generate an email
  - Generate a syslog message to a SIEM
- Quarantine identified threats using the network

Detect and respond to advanced threats

Data hoarding and Data Exfiltration



Reduce incident response time from months to hours

Stealthwatch is available across all deployment methods

Stealthwatch Cloud

Public cloud monitoring

Any business using public cloud infrastructure

Monitors public cloud via SaaS

Complements Cisco Enterprise and Private Network offering

Private network monitoring

SMB & commercial companies

Monitors private network via SaaS

Complements Cisco public cloud offering

Stealthwatch On-Prem

On-Prem network monitoring

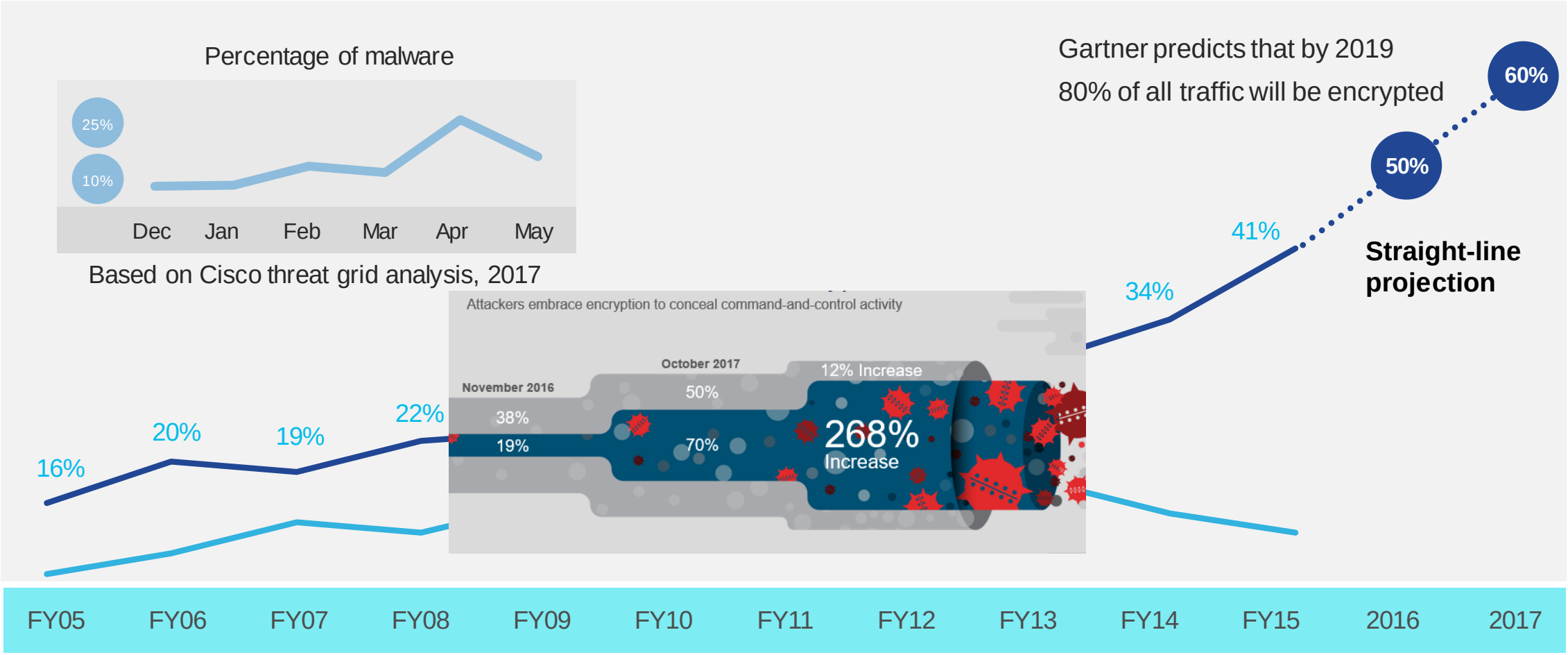
Enterprise & commercial customers

Monitor private network via on-premises virtual or hardware appliance

Complements Cisco public cloud offering

Encrypted Traffic Analytics

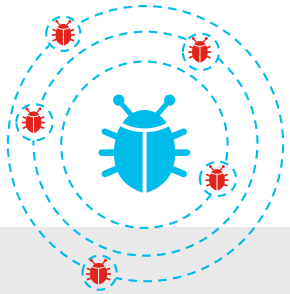
Encryption is changing the threat landscape



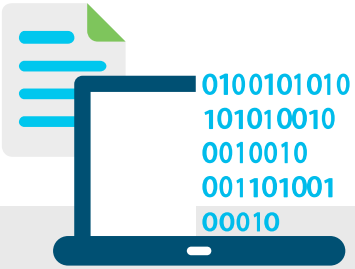
Source: Thales and Vormetric

Encrypted Traffic Analytics

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



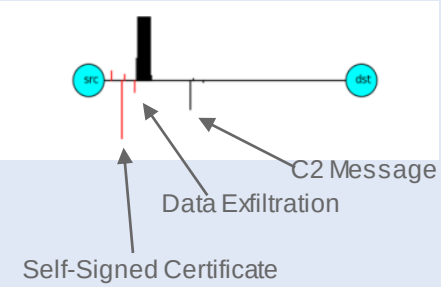
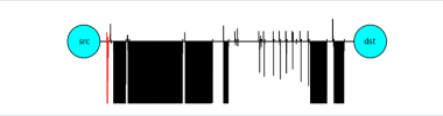
Detect malware in encrypted traffic



Ensure cryptographic compliance

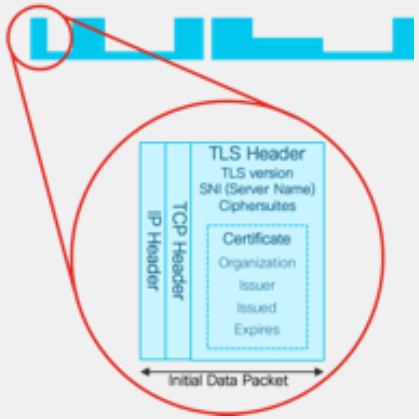
ETA studied Internet encrypted data features

Cisco research

	TCP/IP	DNS	TLS	SPLT
Malware traffic	Watchlist address	c15c0.com afb32d75.com	Unusual fingerprint Unusual cert	 Bestafera
Benign traffic	Prevalent address	cisco.com	Typical fingerprint Typical cert	 Google search

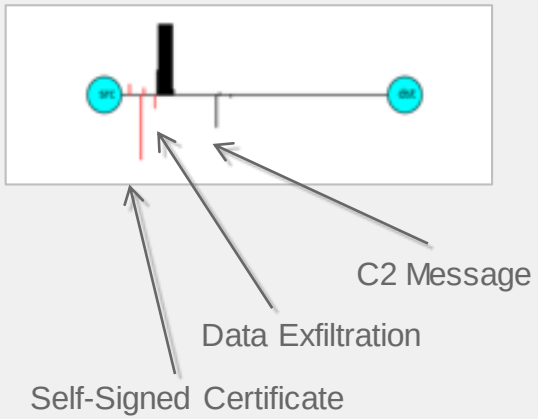
Detect malware in encrypted traffic

Initial data packet



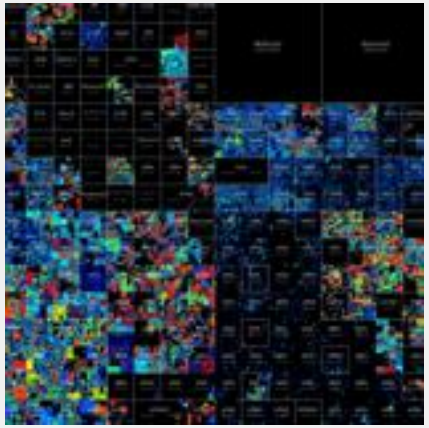
Make the most of the unencrypted fields

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

What is Mobile World Congress?

MOBILE WORLD CONGRESS

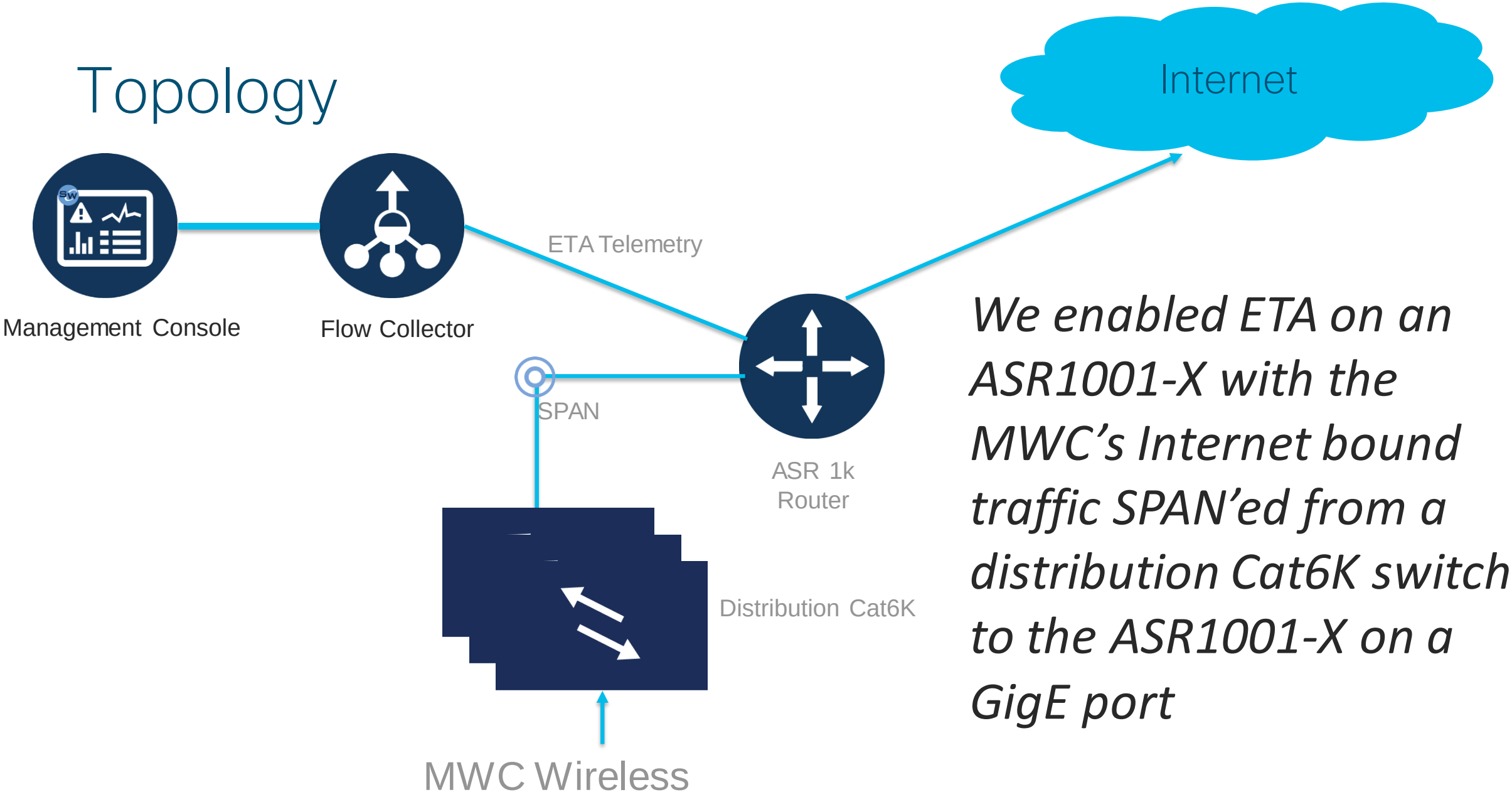
BARCELONA 26 FEB-1 MAR 2018

More than 107,000 visitors from 205 countries and territories

Over 55% of attendees held senior-level positions, including more than 7,700 CEOs

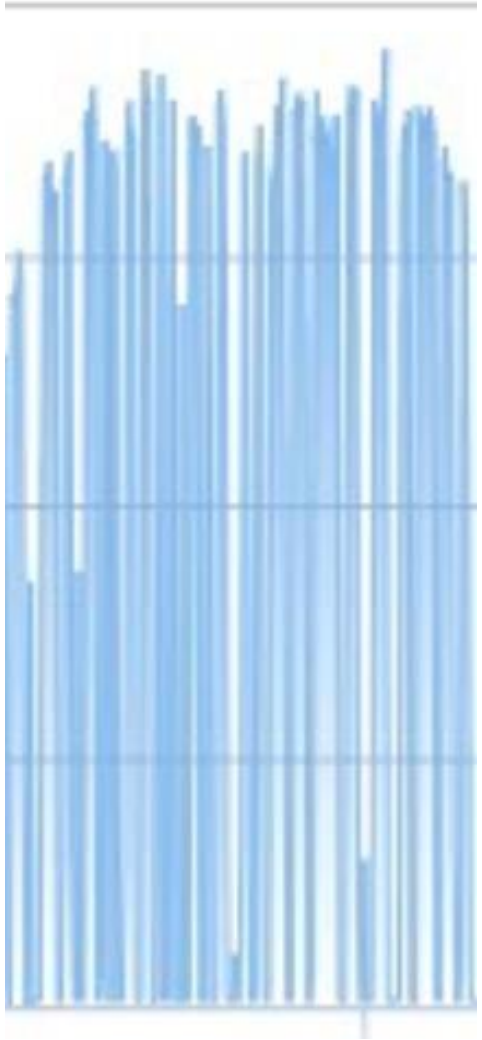
Stealthwatch monitored all the wireless traffic to and from the Internet with Encrypted Traffic Analytics

Topology



We enabled ETA on an ASR1001-X with the MWC's Internet bound traffic SPAN'ed from a distribution Cat6K switch to the ASR1001-X on a GigE port

Summary of the traffic



Sustained flow consumption at ~20k/FlowsPerSecond

More than 55 million flows captured

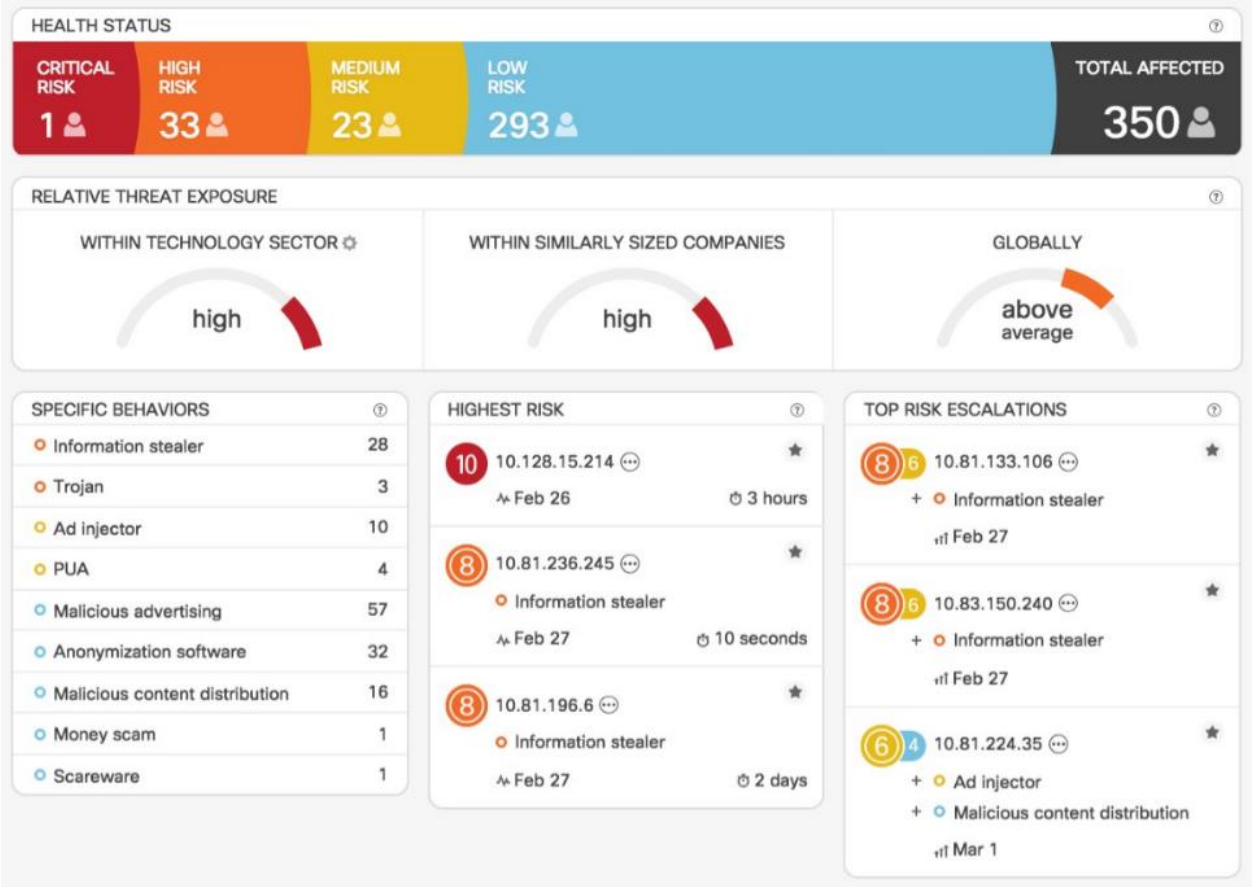
- More than 29 million TCP Sessions
- More than 23 million UDP Sessions
- More than 1.8 million ICMP Sessions

Over a million streaming audio/video application
Over 850,000 flows of P2P file transfer

82% of all the web traffic was encrypted!
(19.5 million HTTPS flows, 3.5 million HTTP flows)

Over 30 applications detected to be using TLS1.0!

Detection on 2/26 and 2/27



Global Threat Analytics raised 350 events

Cryptomining
Android Trojans (Android.spy, Boqx, infected firmware)
SALITY malware
SMB Service discovery malware
OSX Malware Genieo
Conficker
RevMob
Phishing
AdInjectors
Several Android mobile devices were identified to have an infected firmware

Malware Trojans were identified that were **using PowerShell to communicate to the C&C servers through HTTPS**.
Several malwares / potentially unwanted applications that **used Encrypted traffic**

** Over 13,500 alarms in Stealthwatch on 2/26*
Over 18,500 alarms on 2/27

What is needed for ETA?

Licensing, packaging…

Solution Element	Software Version	License
Enterprise switches (Cisco® Catalyst® 9000 Series)*	C9300: Cisco IOS® XE 16.6.1 C9400: Cisco IOS® XE 16.6.2 (Oct)	Included in Cisco DNA™ Advantage license/ Cisco ONE™ Advantage
Branch routers (ASR 1000 Series, 4000 Series ISR, CSR, ISRv)**	Cisco IOS® XE 16.6.2 (Oct)	Included in SEC/k9 license
Stealthwatch® On-prem	v6.9.2 (Available now)	Management Console, Flow Collector, Flow Rate License
Stealthwatch® On-prem	v6.9.2 Cryptographic compliance (Q3CY17) Malware Detection (Q4CY17)	

*Software support for C9500 is current on roadmap.
**Available for Proof of Concept (PoC) with 16.6.1, General availability in 16.6.2 (Oct)

Cisco Stealthwatch Cloud

Technical Decision Maker

Stealthwatch Cloud

Public cloud monitoring	**Private** network monitoring
Any business using public cloud infrastructure	SMB & commercial companies
Monitors public cloud via SaaS	Monitors private network via SaaS
Complements Cisco Enterprise and Private Network offering	Complements Cisco public cloud offering

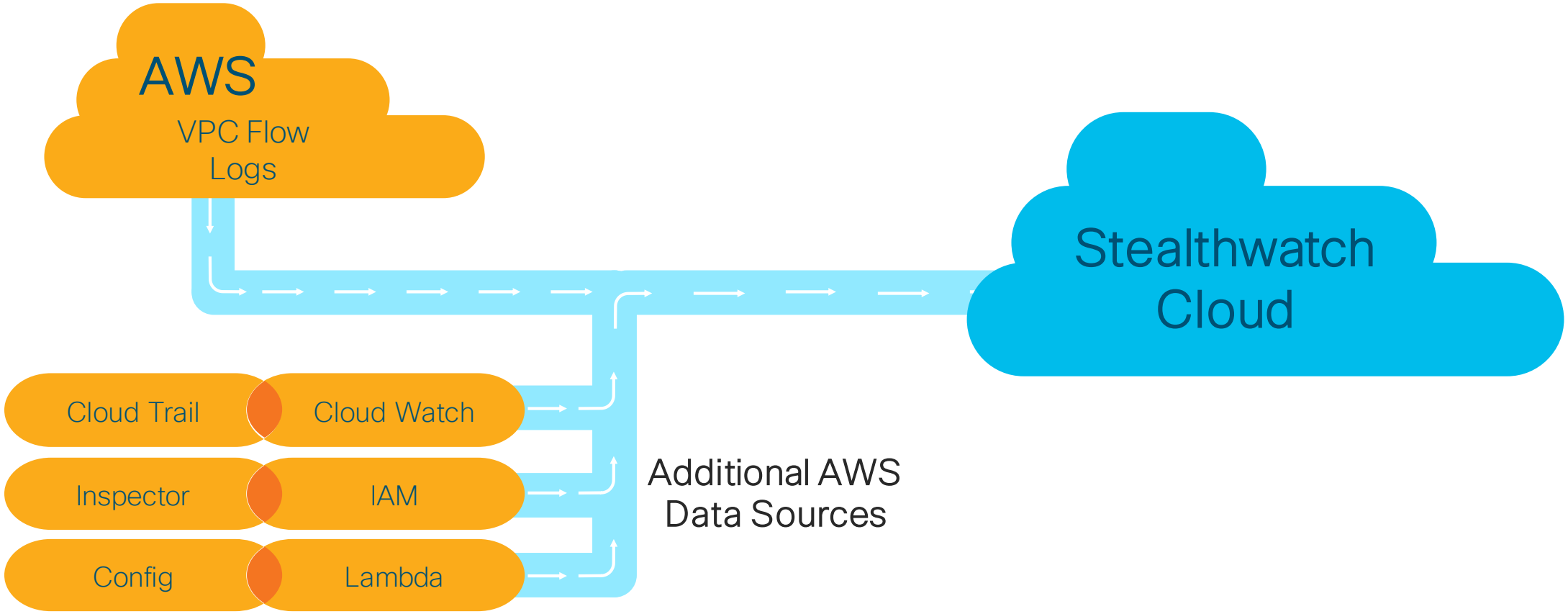
Quick and easy security for dynamic environments

- VPC Flow Logs
- Other data sources

- NetFlow
- Mirror port
- Other data sources

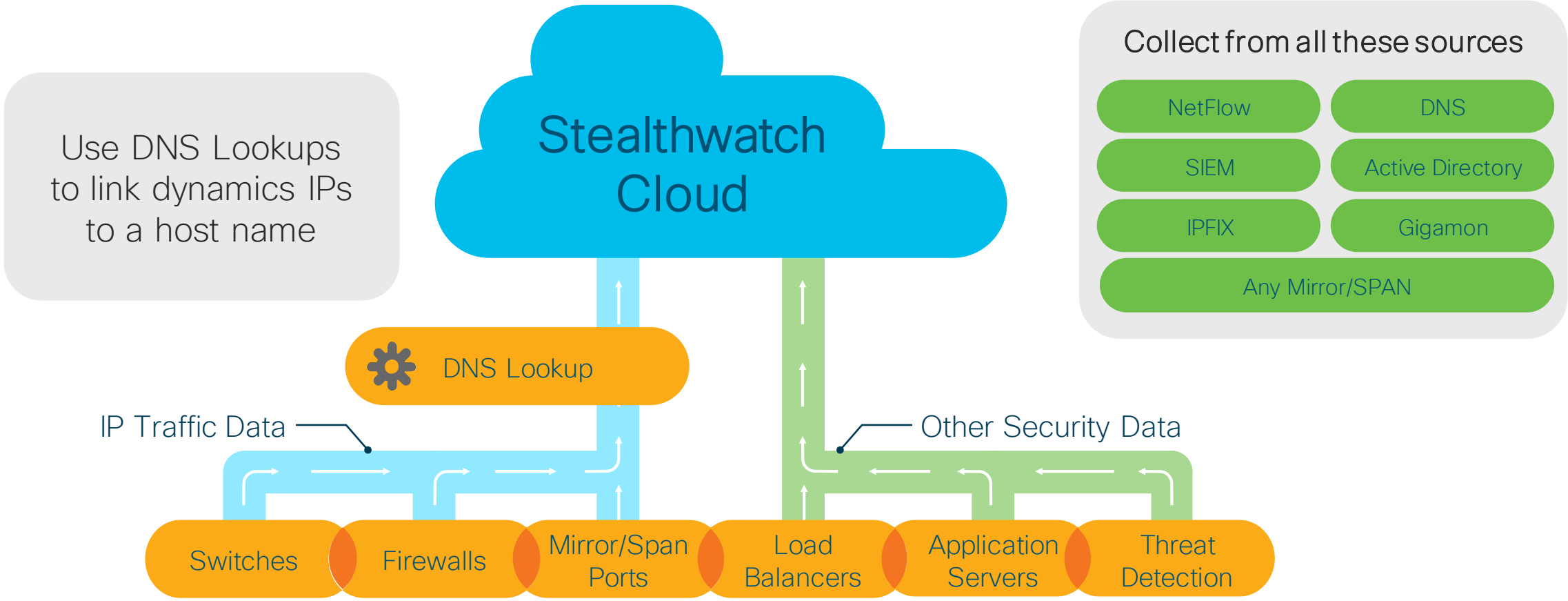
Cover your *entire* cloud attack surface with ease

AWS Flow Logs



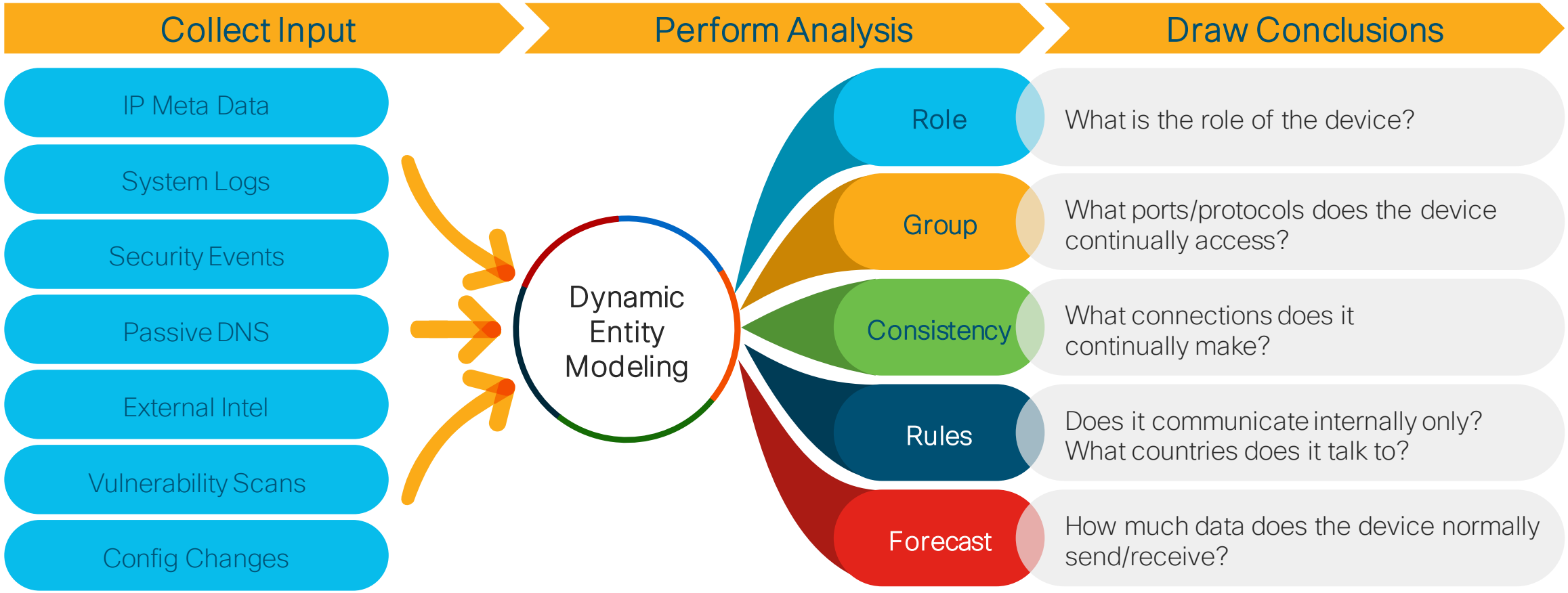
Detect threats and see network activity using existing telemetry sources

Virtual Sensors



Using modeling to detect security events

Dynamic Entity Modeling



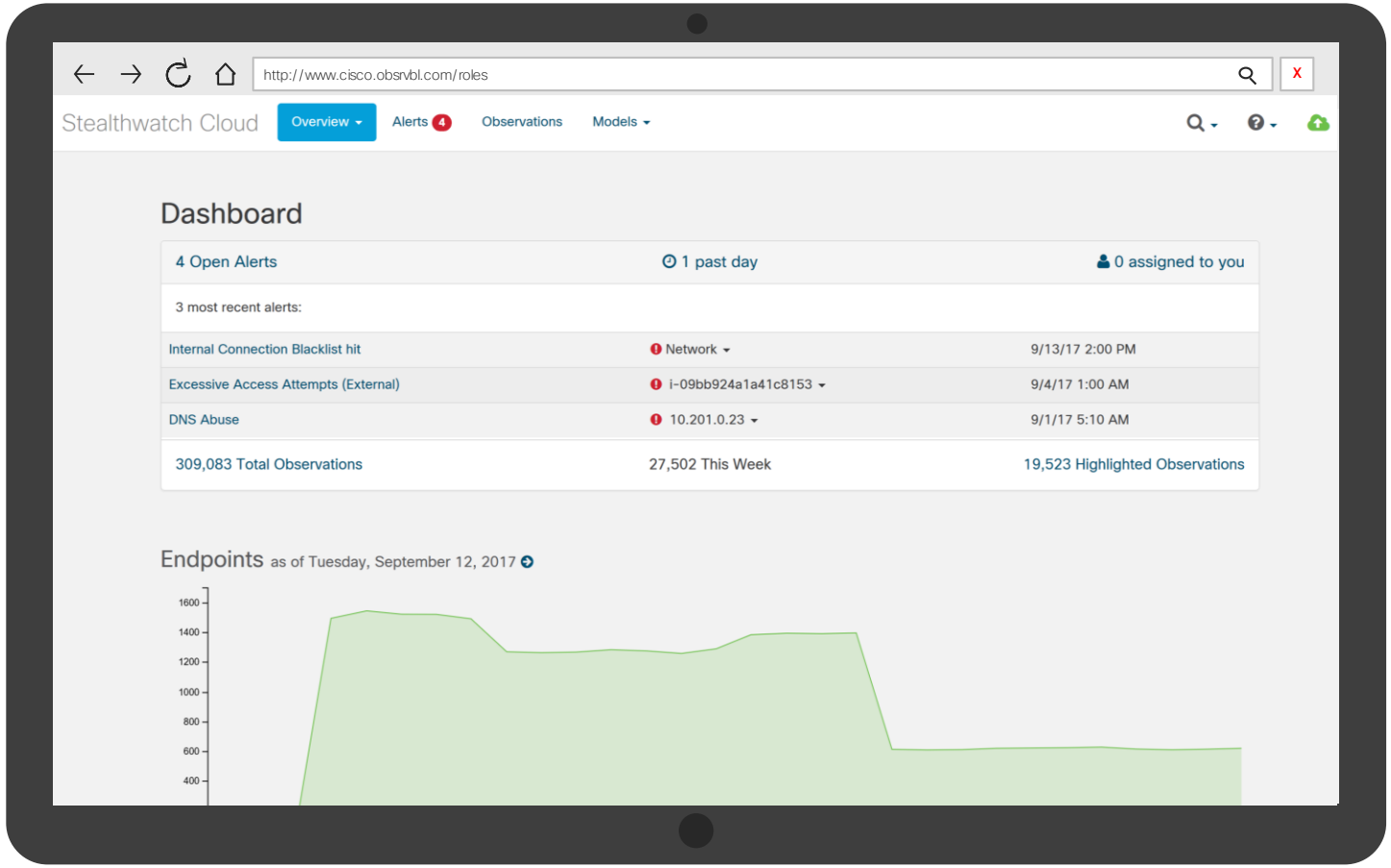
Get the full benefit of the cloud

SaaS-based security

- Easy to use and deploy
- Centrally managed
- Flexible pricing
- Secure data storage
- Automatically scale

Manage everything from a simple SaaS portal

SaaS Management Portal



- Unlimited users
- No patching necessary
- Available anywhere
- New features added monthly
- Support available

Start today with a free 60-day trial

Schedule consultation with a security specialist

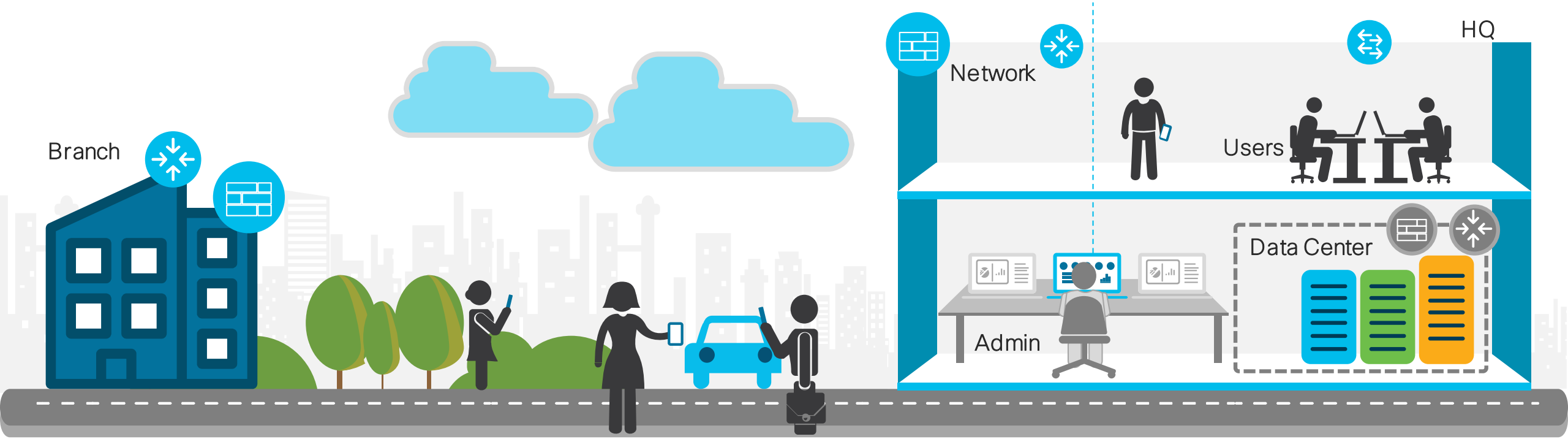
See results within hours

Learn more: cisco.com/go/stealthwatch-cloud

Security Online Visibility Assessment

Are you compromised today?

- What are your risk areas?



Common areas of risk

- Largest risk areas are often things you think are already covered
- Lack of visibility allows risky activity to continue

Can you see…

- ☐ Threats in encrypted traffic
- ☐ Server message block (SMB) traffic
- ☐ Risky DNS traffic
- ☐ Remote access breaches
- ☐ Unclassified and unknown internal servers
- ☐ Internal and external telnet activity
- ☐ Traffic to high risk countries

Cisco Security Online Visibility Assessment

A free, 14-day risk assessment

Focused on common areas of security risk

Provides an immediately actionable, detailed report

The Report

- Detailed results
- Can identify areas of risk and active threats
- Provide actionable intelligence to help you adjust security policies and guide purchase decisions

DNS Risk

Overview

DNS servers are critical to normal network function as they translate URLs to IP addresses. Many organizations utilize specific DNS servers to safeguard their network and enforce policies. When a host is found to be using an unauthorized DNS server, it could indicate malicious activity or policy violation. Malware may change a host's DNS server to forward request to sites used for phishing or exploit delivery. Likewise, network users may utilize unauthorized DNS servers to access web resources forbidden by internal policies.

Unauthorized DNS servers can:

- Direct hosts to bad websites to download malware or exploitation tools
- Prevent monitoring of DNS traffic for data loss, command and control activity and exploitation
- Control or block access to software updates from vendors

Notes

Deploying Cisco Umbrella will allow for better protecting DNS traffic and preventing DNS hijacking.

Unauthorized DNS Servers

DNS SERVER	BYTES	CLIENTS	FLOWS
198.6.1.162	719.1 MB	3	42887
192.175.48.6	682.6 MB	3	40060
192.175.48.42	661.6 MB	3	38690
198.6.1.210	540.8 MB	3	32910
192.102.198.240	243.4 MB	3	32632

Potential Hosts at Risk of Exposure, DNS Malware, or Data Loss

HOST	BYTES	CLIENTS	FLOWS
209.182.184.2	4.5 GB	14477	4599824
10.201.0.16	3.5 GB	14432	3618404
10.10.30.16	1.5 GB	9499	1578488
10.10.30.15	83.3 MB	4	56878
209.182.185.222	471.1 kB	4	644

Ready to start?

Schedule consultation
with a security specialist

Learn more: cisco.com/go/stealthwatch-
free-assessment