



SINOG

Behaviour and anomaly detection

Vedran Franjić, System Engineer Sales

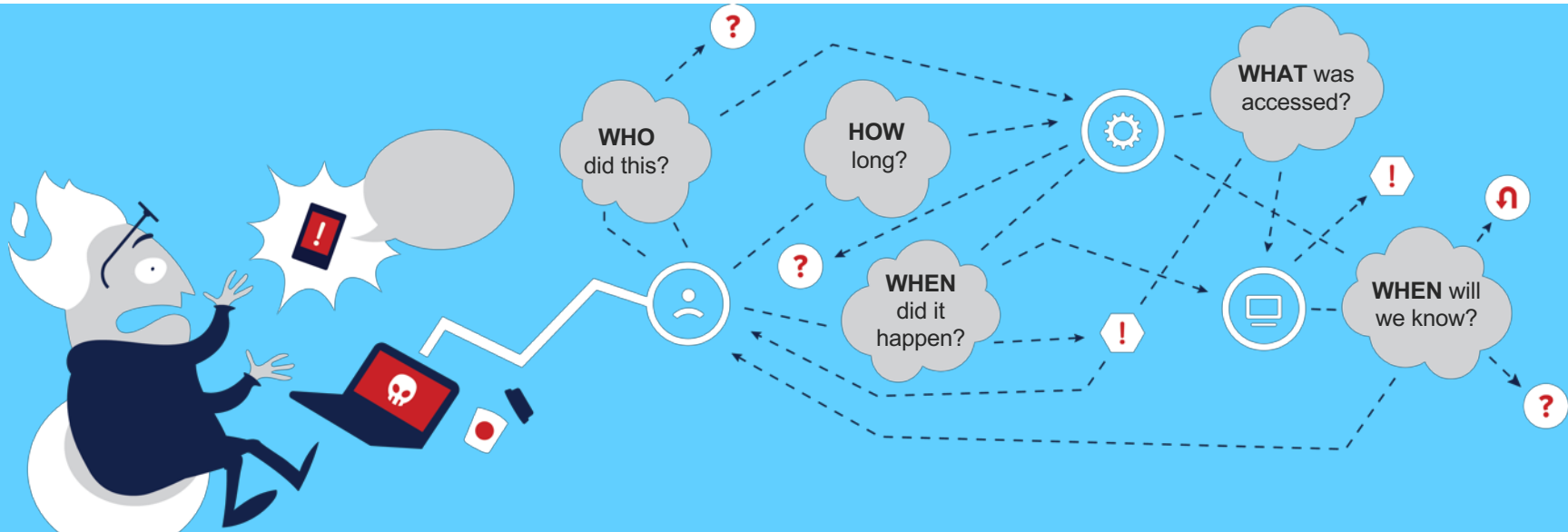
vfranjin@cisoo.com

Agenda

- Common Network Problem
- Stealthwatch Overview
- Use Cases

NO VISIBILITY + NO SECURITY

“internal network traffic”



Effective security depends on total visibility



SEE
every conversation



KNOW
every host



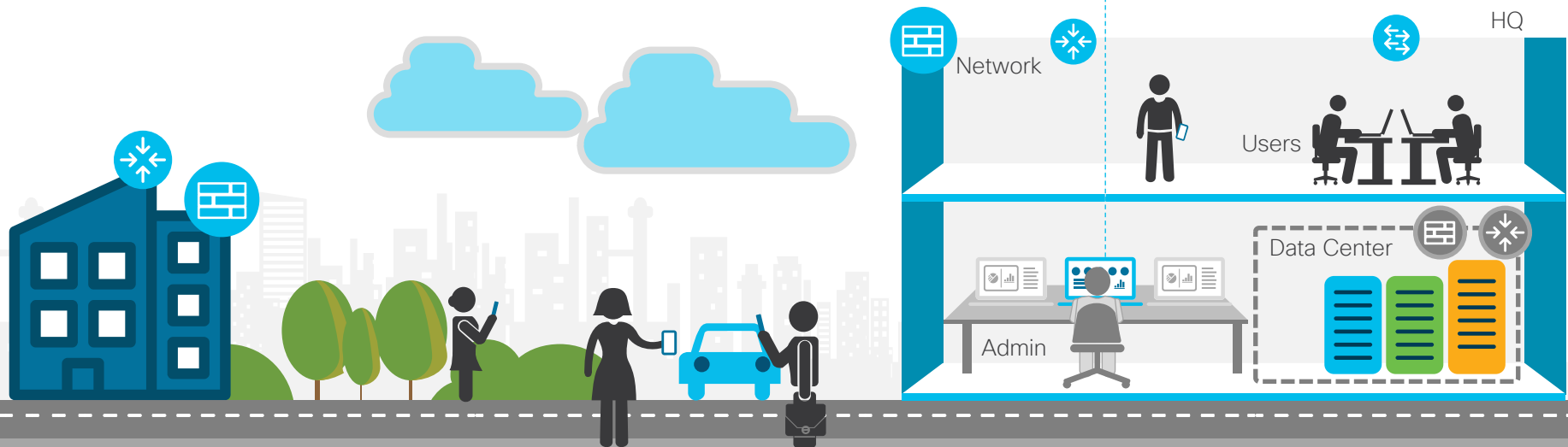
Understand what
is **NORMAL**



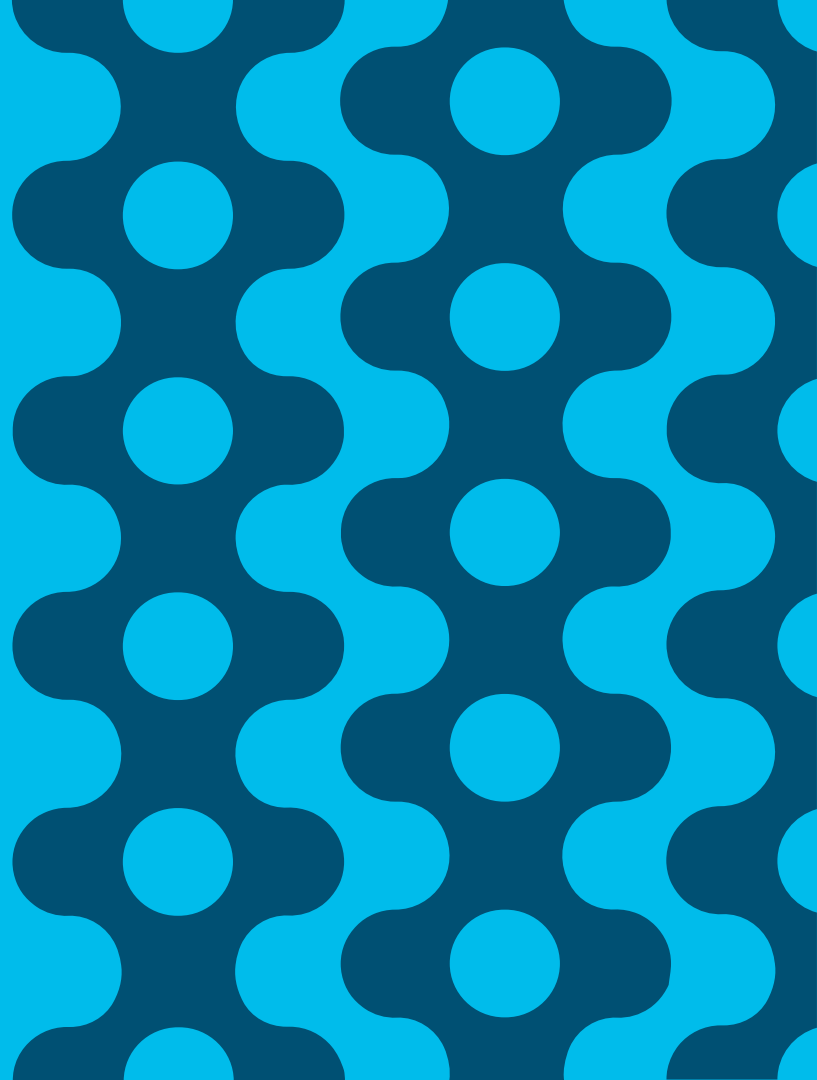
Be alerted to
CHANGE



Respond to
THREATS quickly



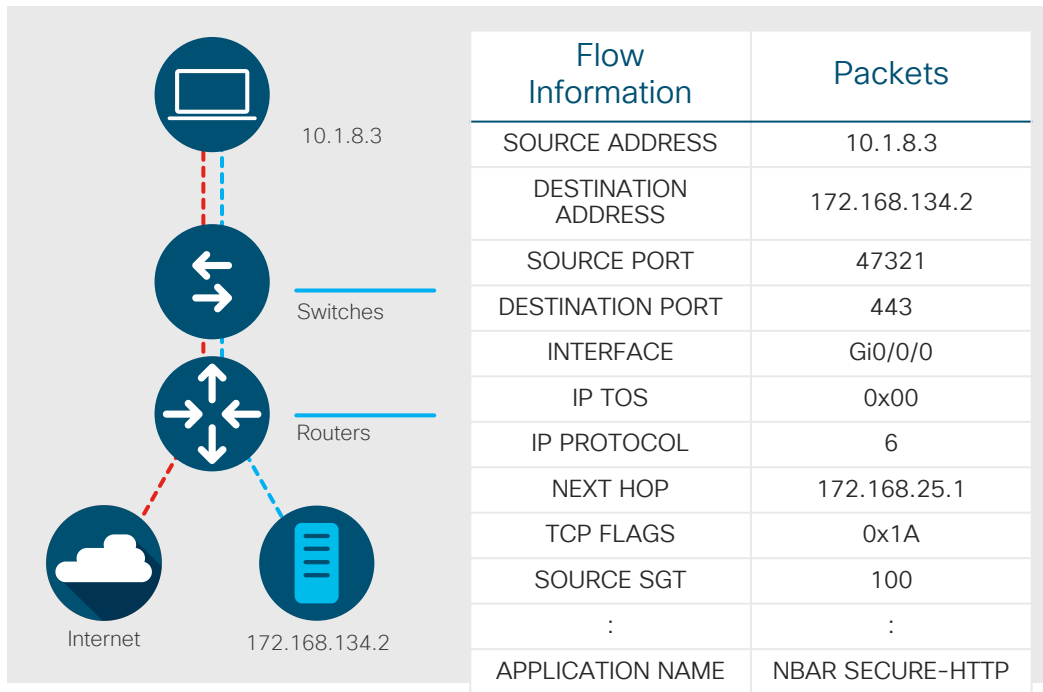
Stealthwatch Overview



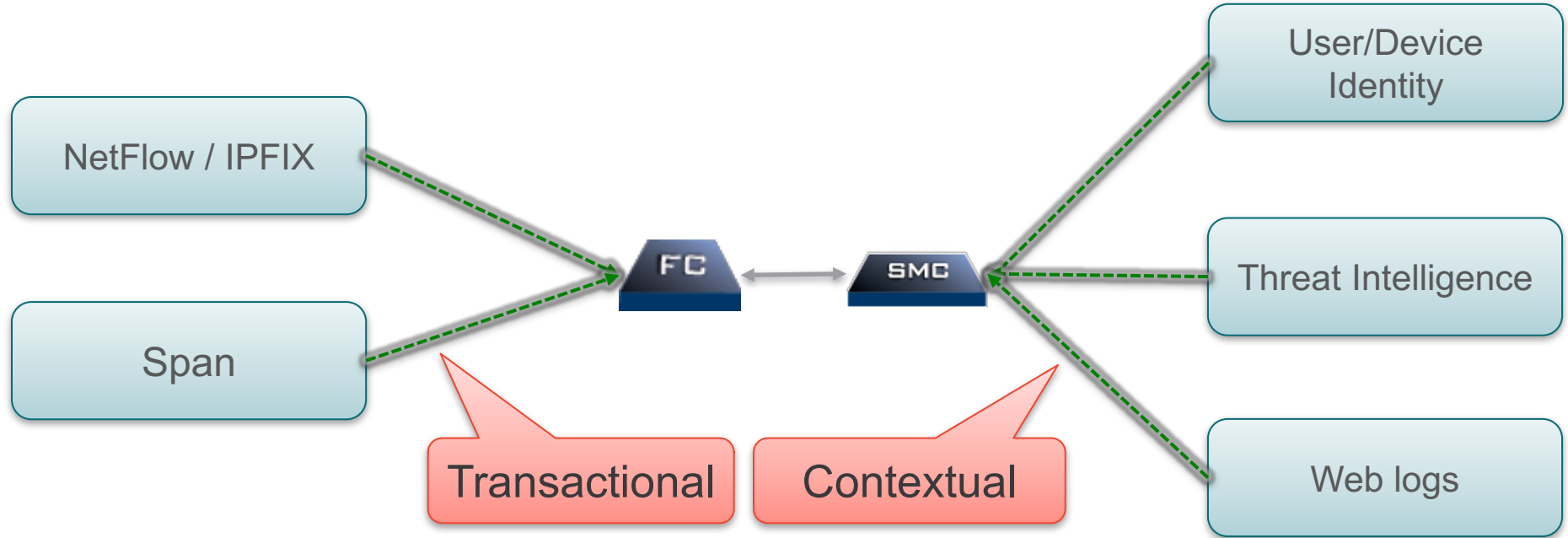
Network as Data Source

Collecting data:





- Collect data across almost every device in your network
- Protocol : NetFlow, sFlow, IPFIX, NSEL, SPAN
- Ability to view north-south as well as east-west communication



Telemetry



Conversational Flow Record

Duration	Who	Search Subject	Port	Traffic S	What	Port	Peer	Who
Start: 05/29 - 12:19:18 PM End: 05/29 - 12:20:58 PM Duration: 1m 40s		 10.10.18.102  RFC 1918 employee1 00:50:56:b4:3f:af	4866/TCP	11.49KB 285 packets	→ HTTP ←	80/TCP	 216.191.247.145  Canada crl.entrust.net	
				1.62MB 1.15K packets				

Flow Detailed Summary: 10.10.18.102

Search Subject Details

Packets: 285
Packet Rate: 2.85pps
Bytes: 11.49KB
Byte Rate: 117.69bps
Percent Transfer:
0.6879458949171267%
Host Groups: Desktops
TrustSec ID: 100
TrustSec Name: Employees
Payload: GET http://crl.entrust.net
/2048ca.crl

Totals

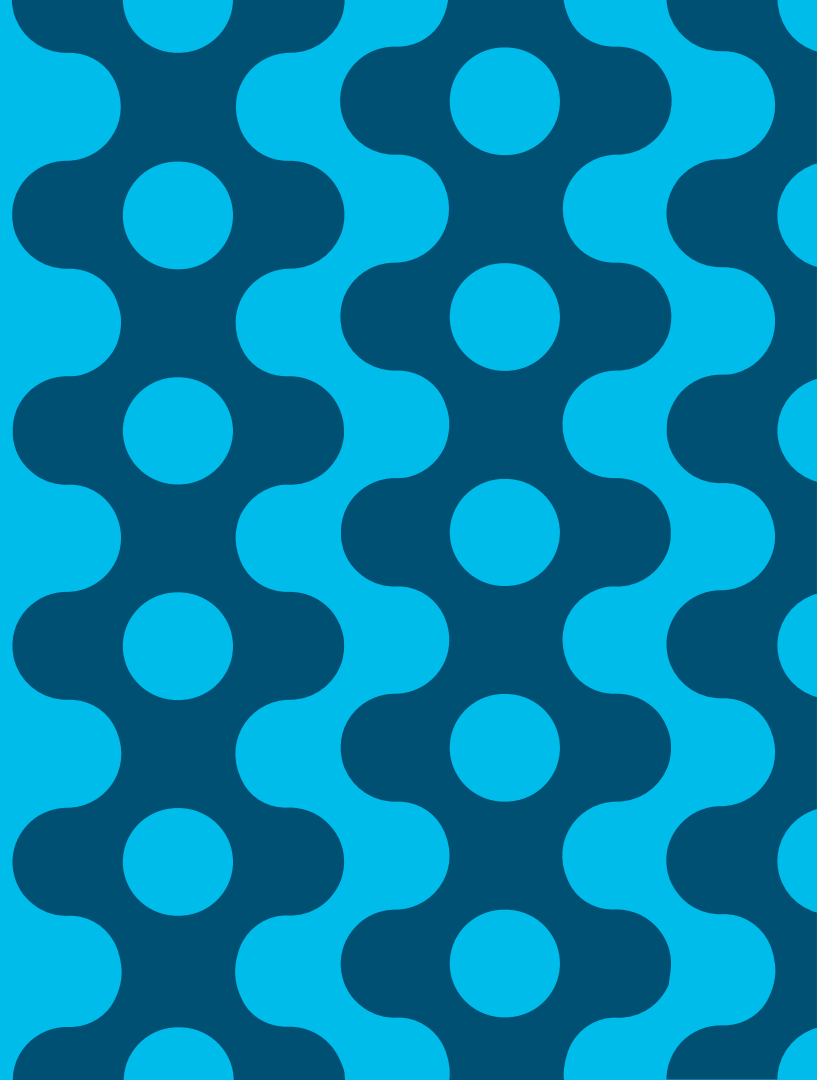
Packets: 1.44K
Packet Rate: 14.37pps
Bytes: 1.63MB
Byte Rate: 17.11Kbps
Search Subject/Peer
Ratio: 0.01
TCP Connections: 2
RTT: 2ms
SRT: 498ms

Peer Details

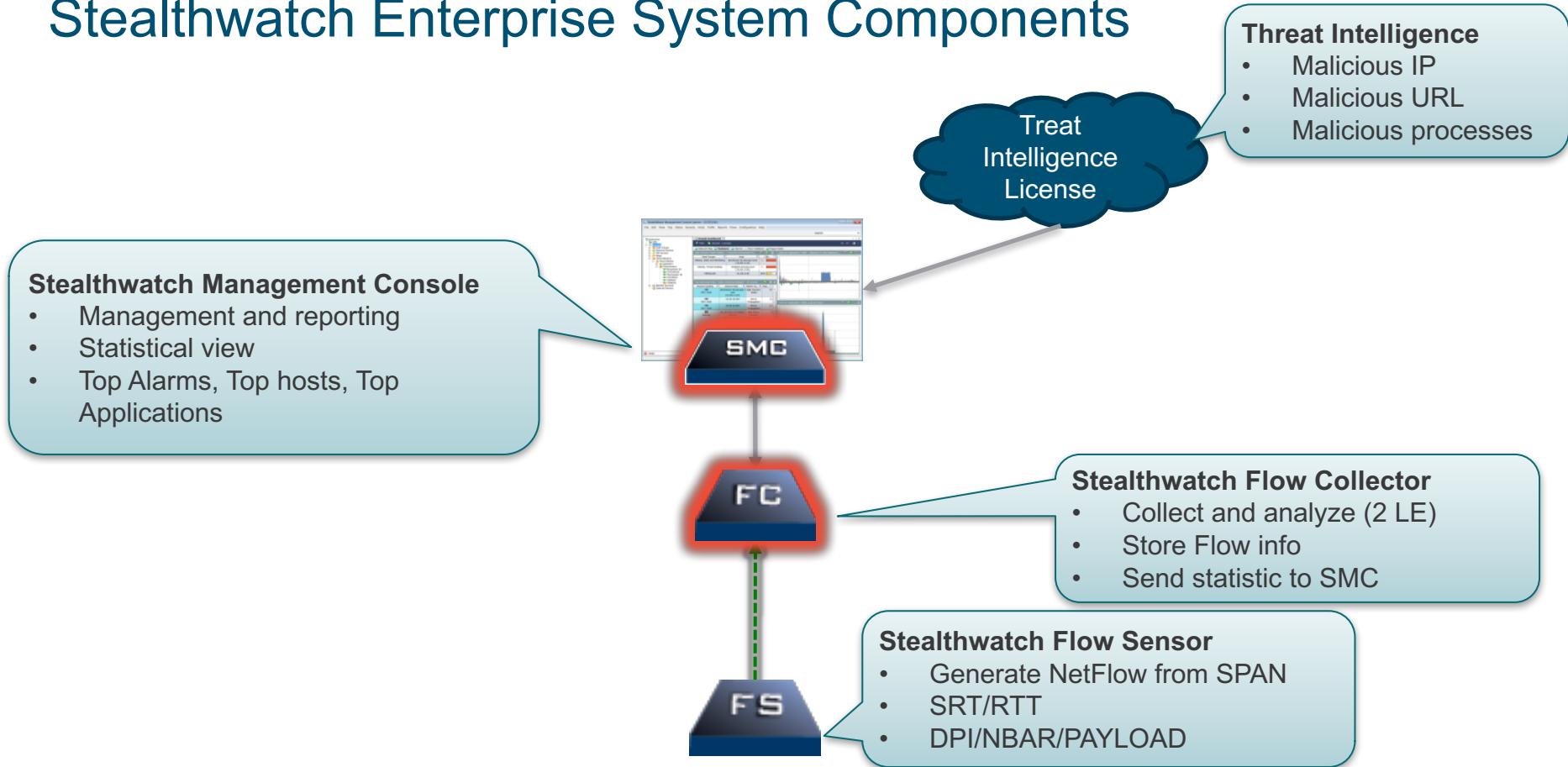
Packets: 1.15K
Packet Rate: 11.52pps
Bytes: 1.62MB
Byte Rate: 16.99Kbps
Percent Transfer:
99.31205410508288%
Host Groups: Canada
Payload: 200 OK
TrustSec ID: 0
TrustSec Name: Unknown

Close

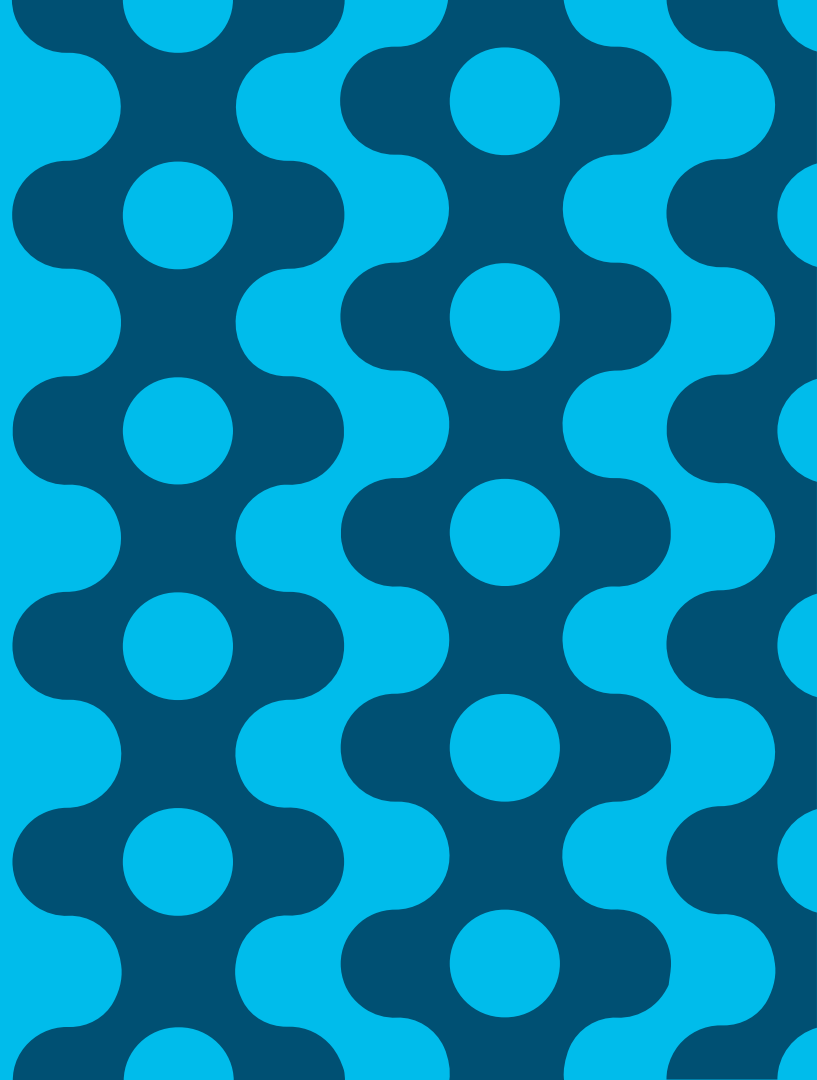
Arhitecture



Stealthwatch Enterprise System Components



Learning engines



Stealthwatch Learning Engines

Stealthwatch

- Behavioural Analysis
- Anomaly detection through statistical learning

Cognitive Analytics

- Cloud Hosted
- Multi-layer Machine Learning
- Anomaly detection through statistical learning
- Encrypted Traffic Analytics
- Malware classification

Top Alarming Hosts	
HOST	CATEGORY
10.201.3.149 ⓘ	DH RC CI EX
End User Devices	
10.201.3.18 ⓘ	DH RC
End User Devices	
10.201.0.23 ⓘ	DH EX
Terminal Servers	
10.150.1.200 ⓘ	RC DH EX CI
WebHostedApp	
10.10.101.24 ⓘ	
End User Devices	

Cognitive Threat Analytics

AFFECTED USERS BY RISK

Critical	High	Medium	Low
1	13	1	1

10

dusti.hilton

Ransomware

ENCRYPTED

9

10.201.3.40

Banking trojan

ENCRYPTED

9

tana.rusin

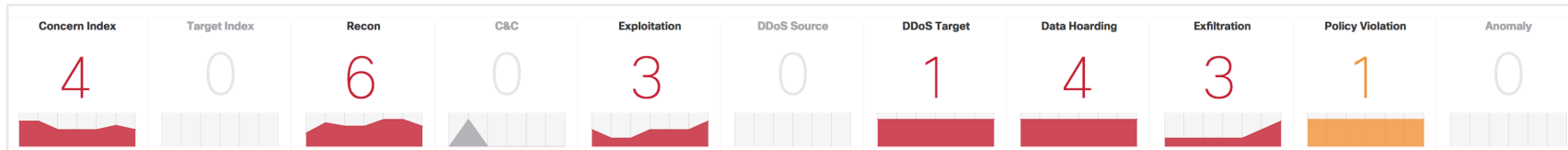
Information stealer, Ad injector

Enterprise

Stealthwatch Enterprise

Logical alarms based on suspicious events

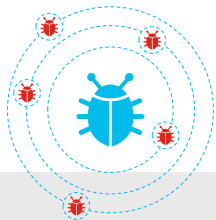
Source or target of malicious behavior	Reconnaissance	Command and Control	DDoS Activity	Insider threats
Scanning, excessive network activity such as file copying or transfer, policy violation, etc.	Port scanning for vulnerabilities or running services	Communication back to an external remote controlling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



Encrypted Traffic Analytics



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

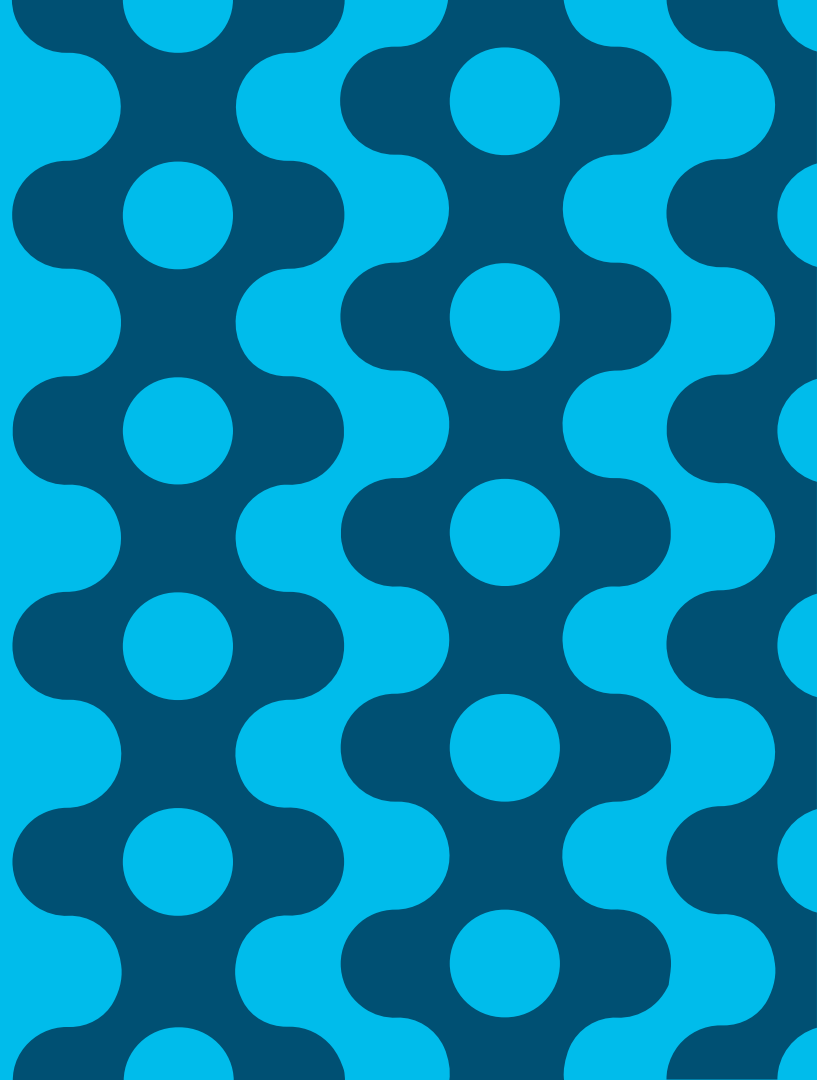


Detect malware
in encrypted traffic



Ensure cryptographic
compliance

USE CASES



Network

- Interface Status Report
- Investigating Slow Network Performance
- Detecting Policy Violations

Security

- Detecting Malware Propagation
- Detect Rogue DNS Traffic
- Detecting Internal Brute Force Attacks
- Alarm Category: Data Hoarding
- Detecting Application Tunneling

[USE CASES ONLINE](#)

Summary

- Using your network as THE 2nd line of defense for enforcement
- You already have the investment
- Agent/endpoint/network agnostic
- No device (example IoT) can hide from the network itself
- Encrypted traffic a non-issue