Cisco Network as a Sensor

A self-learning security sensor and enforcer

Daniel Tulen
WW Channel Team, CSE Advanced Threat Solutions EMEAR
March ‘17

Do we need network based security?

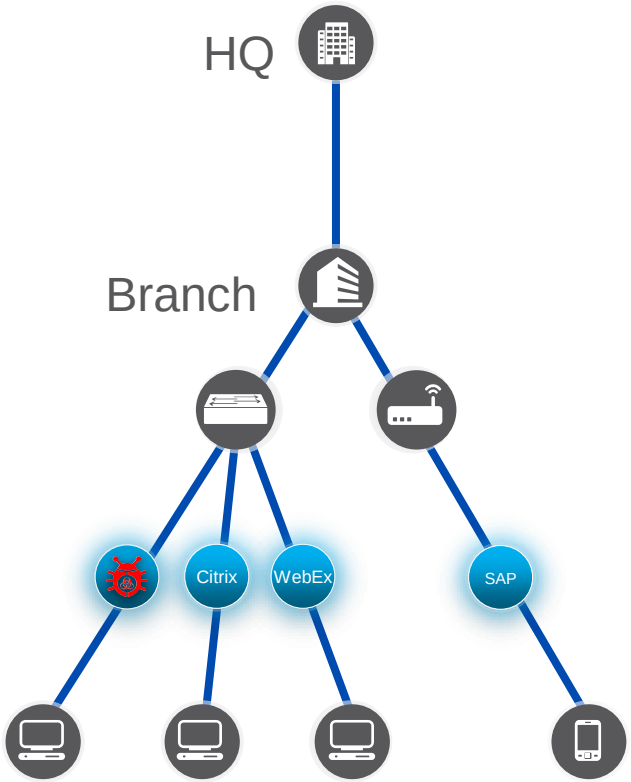
Threats have grown complex, multifaceted, voluminous, easier and cheaper

When we try to keep pace manually, threats will fall through the cracks

Automation is the only way to master network security

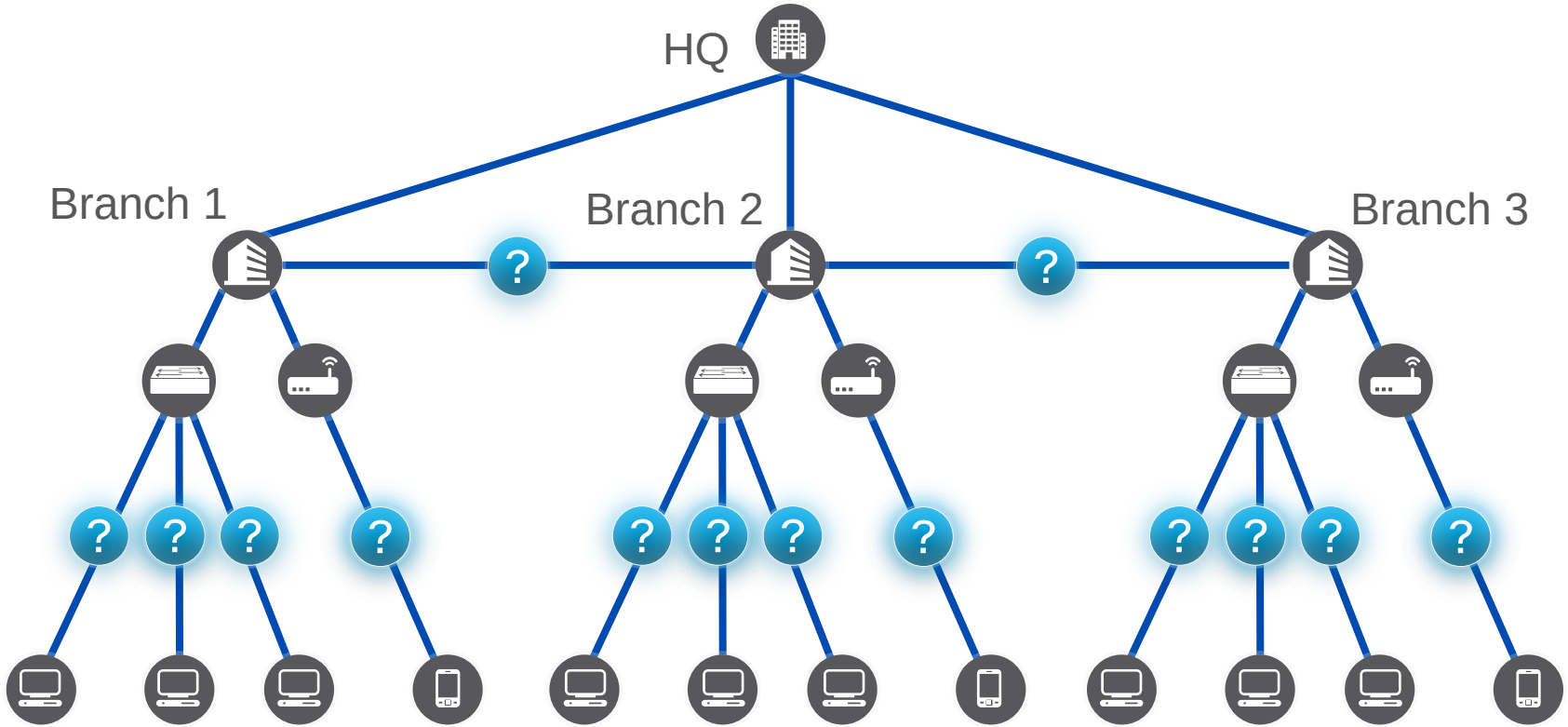
C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

You can’t defend against what you can’t see



C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Distributed networks make it is even harder



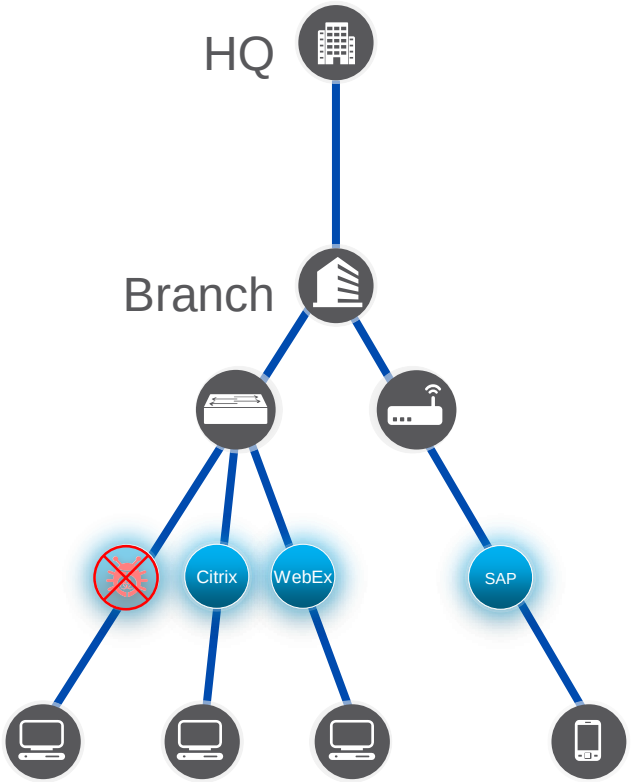
C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security from a network perspective

Network Visibility

Integrated Threat Visibility

Policy Enforcement



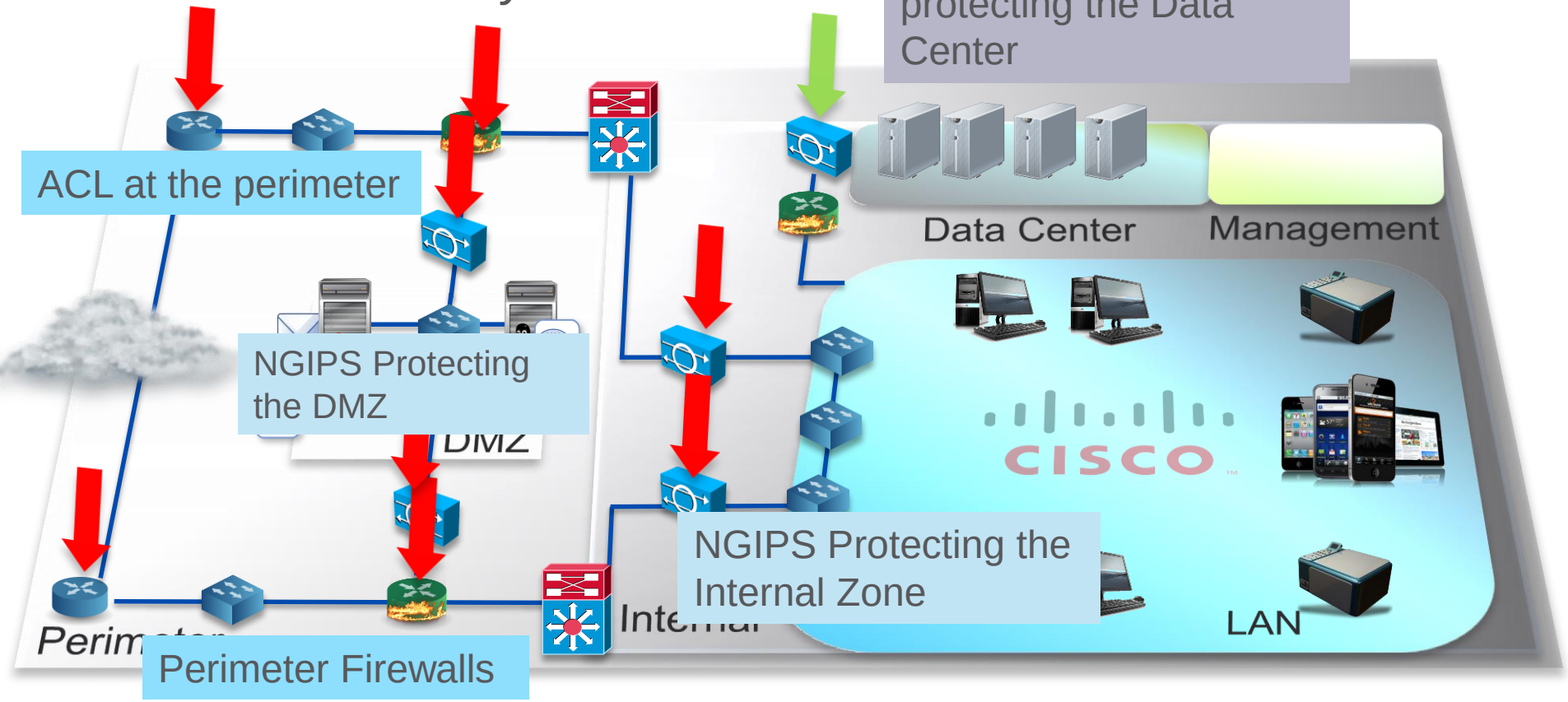
Device Monitoring

Automated Correlation

Network Segmentation

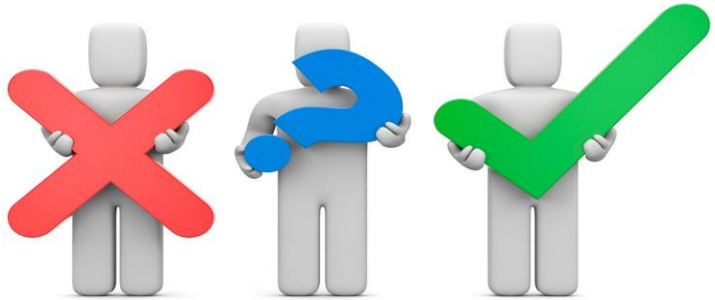
C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Perimeter Security Controls



What are we using today?

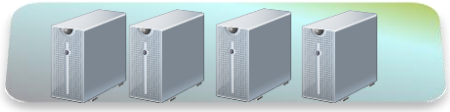
- SNMP
  - Average with an 5 minute interval.
  - Load on CPU
  - Requires often custom MIBS
- SPAN
  - No VLAN and CRC information
  - Oversubscription gets dropped
  - Often max 2 active SPAN ports per device
- SYSLOG
  - Often not detailed
  - High volume of data



C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Missing focus:

- Inside the networks
- Between the security solutions
- The non-inspected traffic
- Everything you forgot about



Data Center

DMZ

LAN

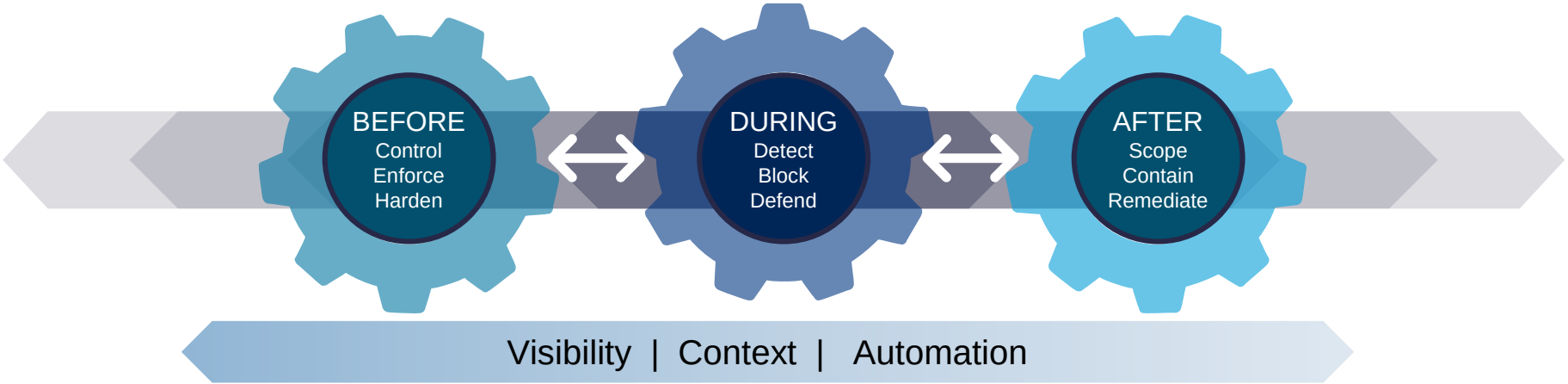
C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Islands of Security

- Am I alone on my Island?
  - What happens on the other side of my island?
  - Are there deadly threats?
  - Am I protected against forces of nature?
- What about neighbors?
  - Do I have neighbors?
  - Can they come to my island?
  - What if they are cannibals?

C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The New Security Model & Network as a Sensor



BEFORE Harden	**DURING** Detect	**AFTER** Scope
Discovery and Classify Assets	Detect Anomalous Traffic	Identify Assets at Risk
Baseline Behavior	Detect Access Policy Violations	Gather Intelligence
Assess Policy and Segmentation		Improve Defenses

C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

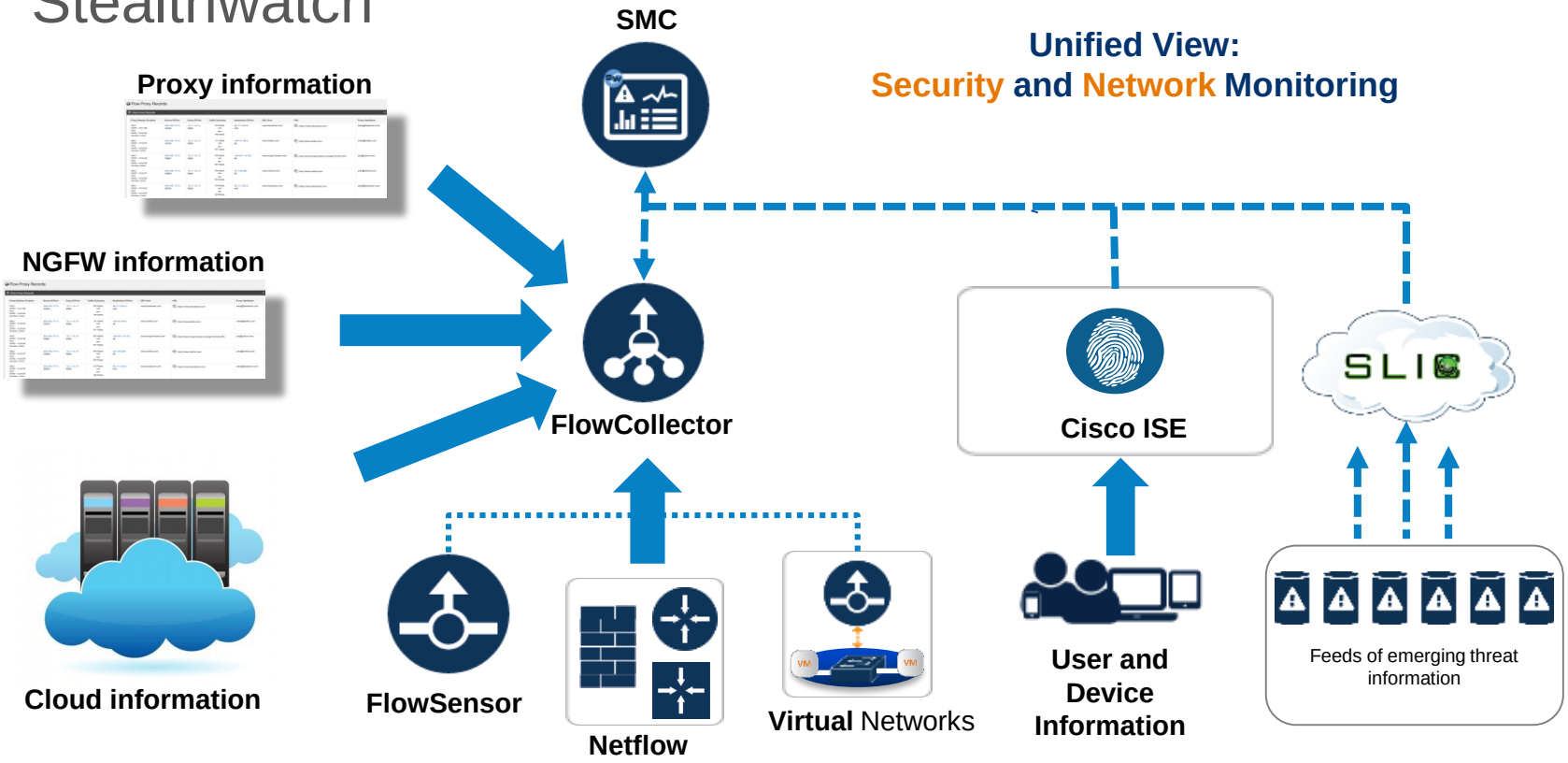
Today's networks require an dynamic security approach…

…to quickly determine what's "normal" within the context of dynamic network variables

…to take automatic action that enforces policy and remediates threats

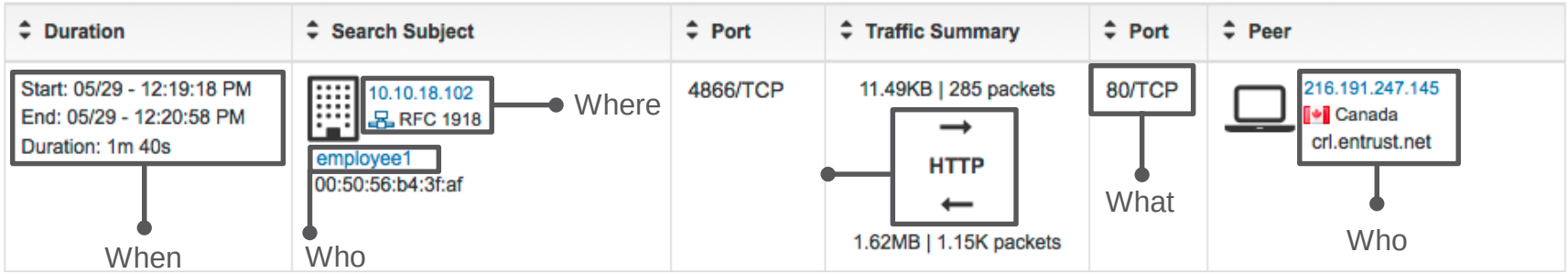
C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Stealthwatch

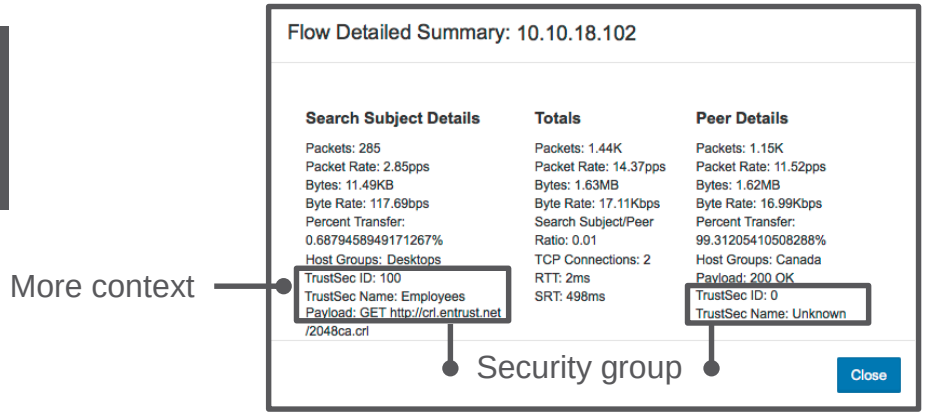


C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Conversational Flow Record



- Highly scalable (enterprise-class) collection
- High compression => long-term storage
  - Months of data retention



C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Turn your network into a security sensor

A Netflow supporting network can:

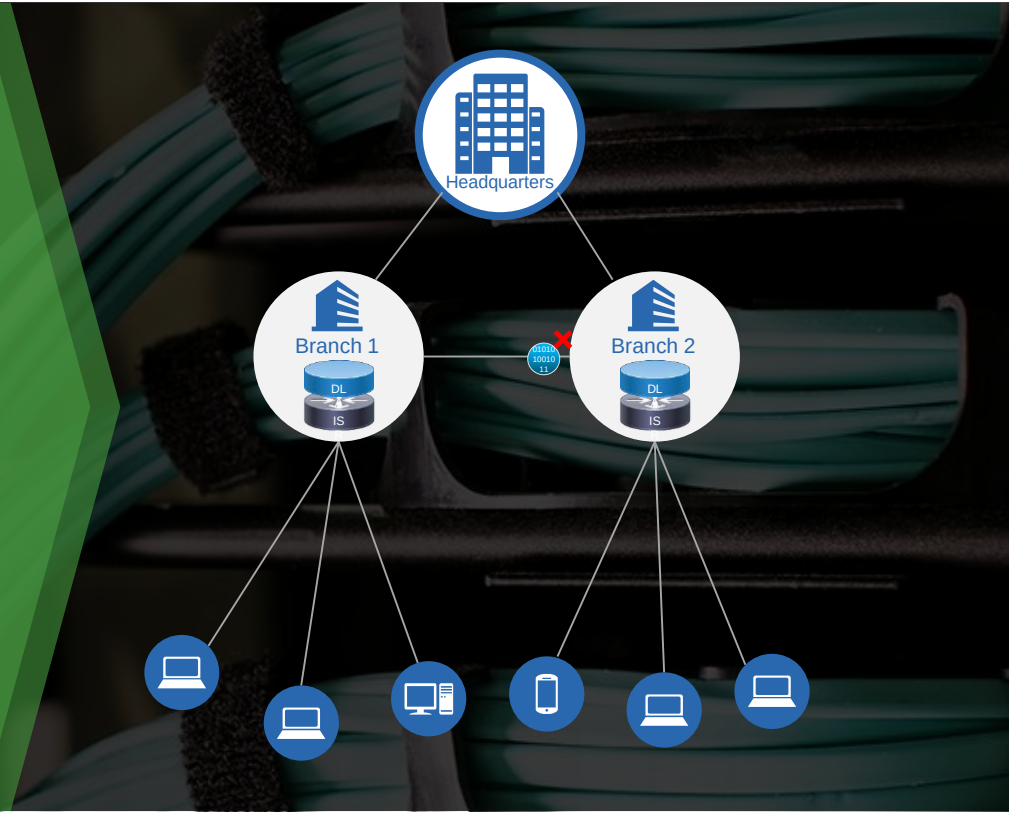
- Monitor all traffic
- Develop traffic patterns and helping developing policies
- Integrate security and network operations
- Report to a single pane of glass

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Detect lateral movement of threats on the network

Lateral movement can be detected or flagged on the network:

- Capture packets
- Identify with application recognition
- Detect anomalies
- Recognize traffic patterns
- Detect threats like malware / DDoS



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Extend security without impacting performance

Enable detection and analyzing every flow, reducing:

- Unnecessary communications within the network
- Processing times for spotting anomalies and threats
- Policy violations
- Performance incidents

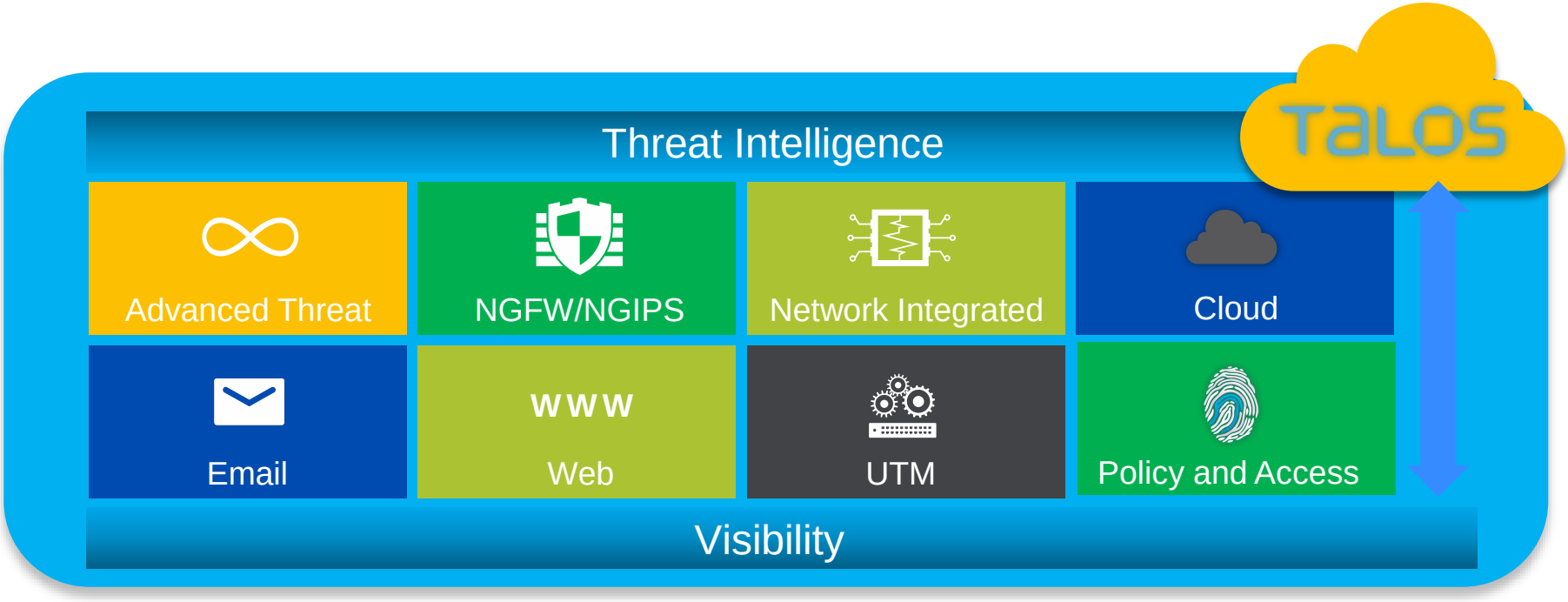
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

But also:

- Rogue Device Detection
- Compliance, Client and Regulator Reporting
- Incident Response
- Insider Threat & Data Loss
- Targeted Attack
- Slow Network
- Because what they had in place failed……

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco’s integrated solution for best threat protection



Best of Breed | Architectural Approach

C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Next Steps

Schedule a meeting with your Cisco Security Sales Rep / SE

Learn more at www.cisco.com/go/Security

C97-737473-00 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO