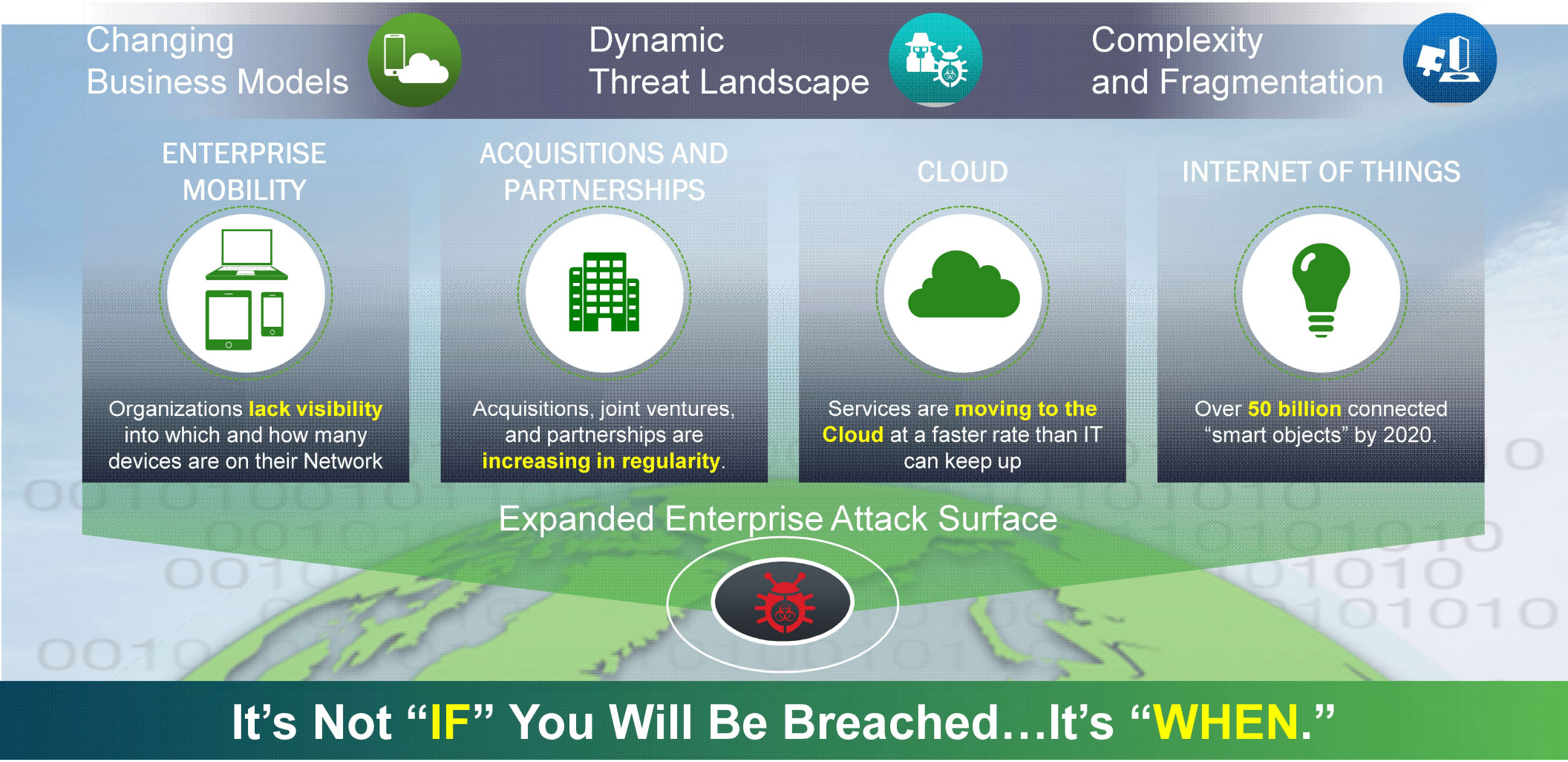
Security for the Digital Age

New Approach for New Challenges

Tim Nan
Business Development Director
Sep 9, 2016

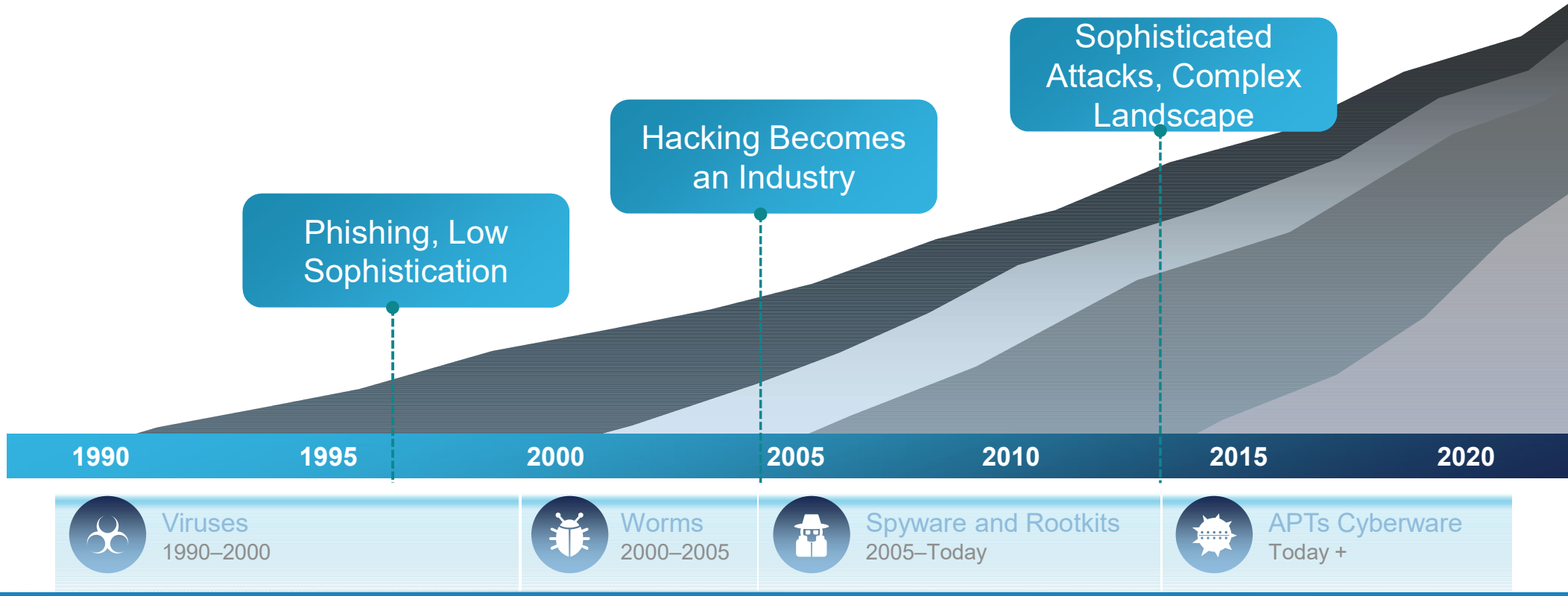
Industry Trends and Business Drivers

New Networks Mean New Security Challenges



It's Not "IF" You Will Be Breached…It's "WHEN."

Network Threats Are Getting Smarter



Criminals Know More About Your Network Than You Do

Custom Malware Remains Dormant for Months to Learn Vulnerabilities in the Network and then Attack those Vulnerabilities.

You Can’t Defend Against What You Can’t See

Cisco’s Threat-Centric Model

Strategic Imperatives

Visibility-Driven

Network-Integrated, Broad Sensor Base, Context and Automation

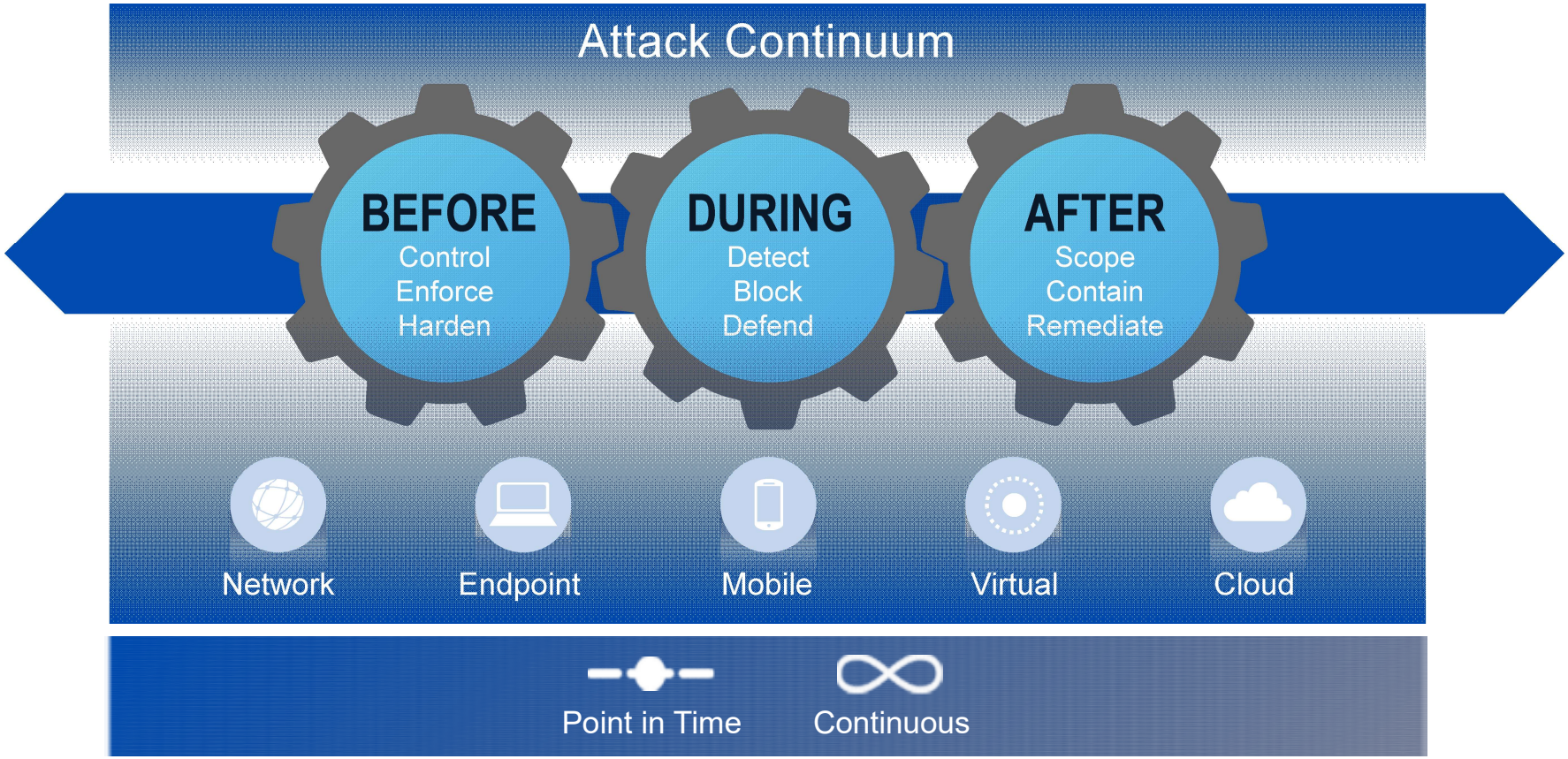
Threat-Focused

Continuous Advanced Threat Protection, Cloud-Based Security Intelligence

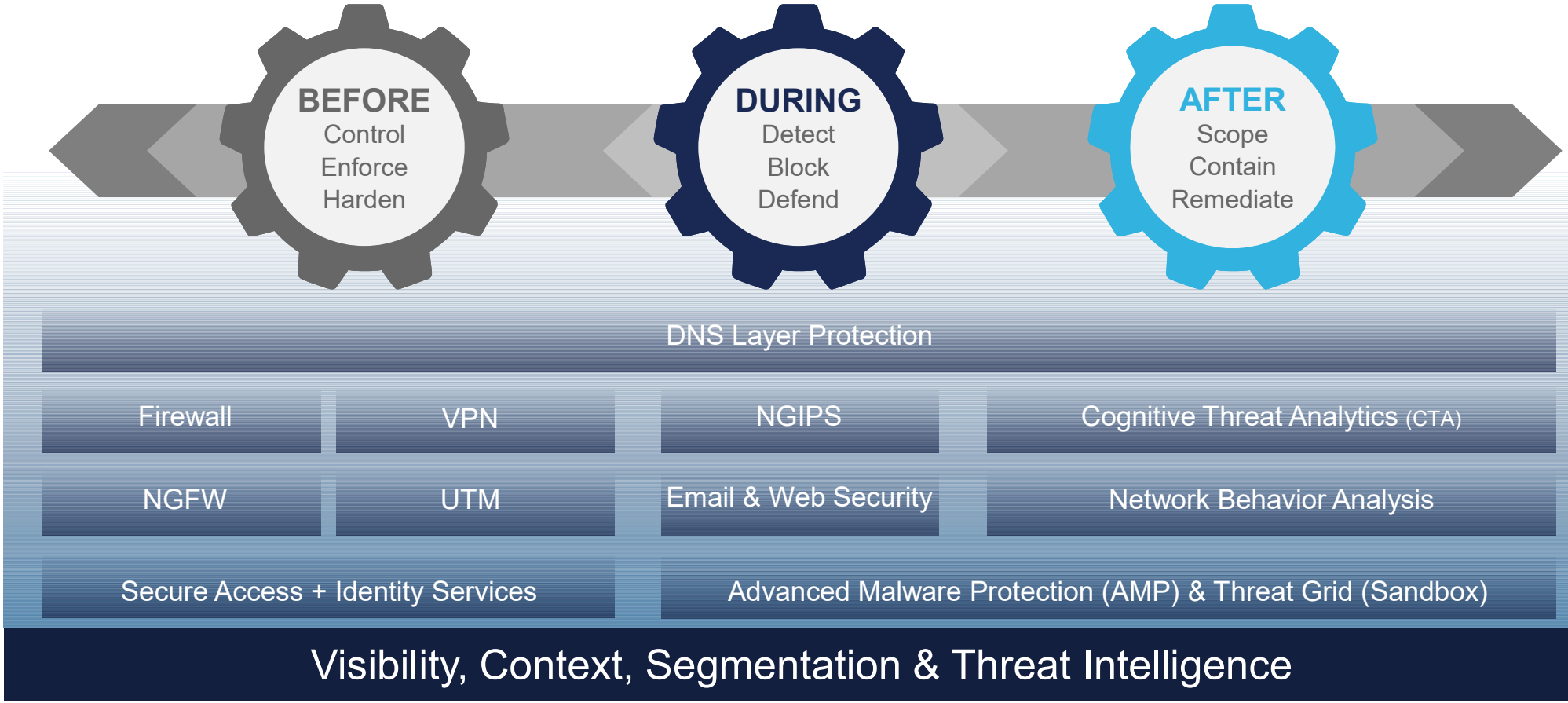
Architecture Focused

Agile and Open Platforms, Built for Scale, Consistent Control, Management

The Cisco Security Model

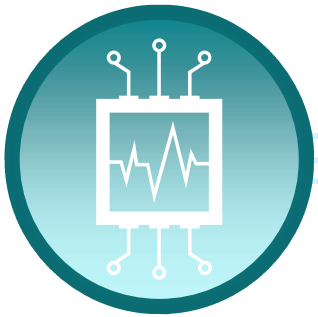


Threat Centric model to cover the Entire Attack Continuum



Network as a Sensor / Enforcer Solution Overview

Cisco Network as a Sensor (NaaS)



Detect Anomalous Traffic Flows, Malware

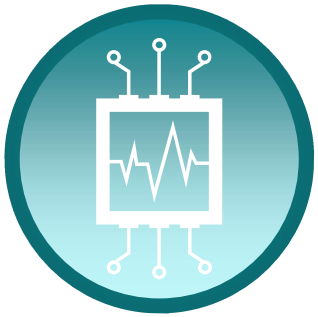
Identify User Access Policy Violations

Obtain Broad Visibility into All Network Traffic

Cisco Network as an Enforcer (NaaE)

- Implement Access Controls to Secure Resources
- Contain the Scope of an Attack on the Network
- Quarantine Threats, Reduce Time-to-Remediation

A Solution Providing Deeper Visibility and Greater Defense against Network Threats



Network as a Sensor (NaaS)

- Cisco Networking Portfolio
- Cisco NetFlow
- Cisco StealthWatch
- Cisco Identity Services Engine (ISE)

Network as an Enforcer (NaaE)

- Cisco Networking Portfolio
- Cisco NetFlow
- Cisco StealthWatch
- Cisco Identity Services Engine (ISE)
- Cisco TrustSec Software-Defined Segmentation

NetFlow for Dynamic Network Awareness

Understand Network Behavior and Establish a Network's Normal

A Powerful Information Source
for Every Network Conversation

Each and Every Network Conversation over an Extended Period of Time

Source and Destination IP Address, IP Ports, Time, Data Transferred, and More

Stored for Future Analysis

A Critical Tool
to Identify a Security Breach

Identify Anomalous Activity

Reconstruct the Sequence of Events

Forensic Evidence and Regulatory Compliance

NetFlow for Full Details, NetFlow-Lite for 1/n Samples

Network Flows Highlight Attack Signatures

StealthWatch System
Network Reconnaissance Using Dynamic NetFlow Analysis

Monitor

- Understand your network normal
- Gain real-time situational awareness of all traffic

Detect

- Leverage Network Behavior Anomaly detection & analytics
- Detect behaviors linked to APTs, insider threats, DDoS, and malware

Analyze

- Collect & Analyze holistic network audit trails
- Achieve faster root cause analysis to conduct thorough forensic investigations

Respond

- Accelerate network troubleshooting & threat mitigation
- Respond quickly to threats by taking action to quarantine through Cisco ISE

Cisco Identity Services Engine (ISE)

Adding Visibility and Context to NetFlow

SEND CONTEXTUAL DATA COLLECTED FROM USERS, DEVICES, AND NETWORKS TO LANCOPE FOR ADVANCED INSIGHTS AND NETFLOW ANALYTICS

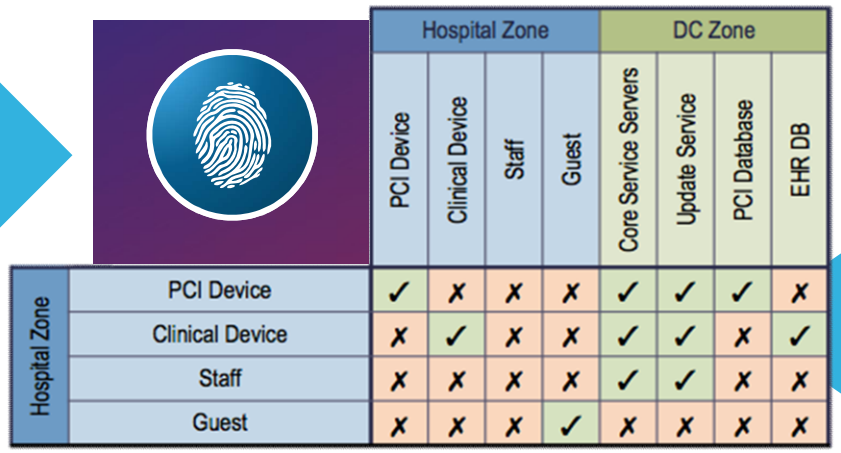
Cisco TrustSec Software-Defined Segmentation

Provide Role-Based Segmentation to Control Access and Contain Threats

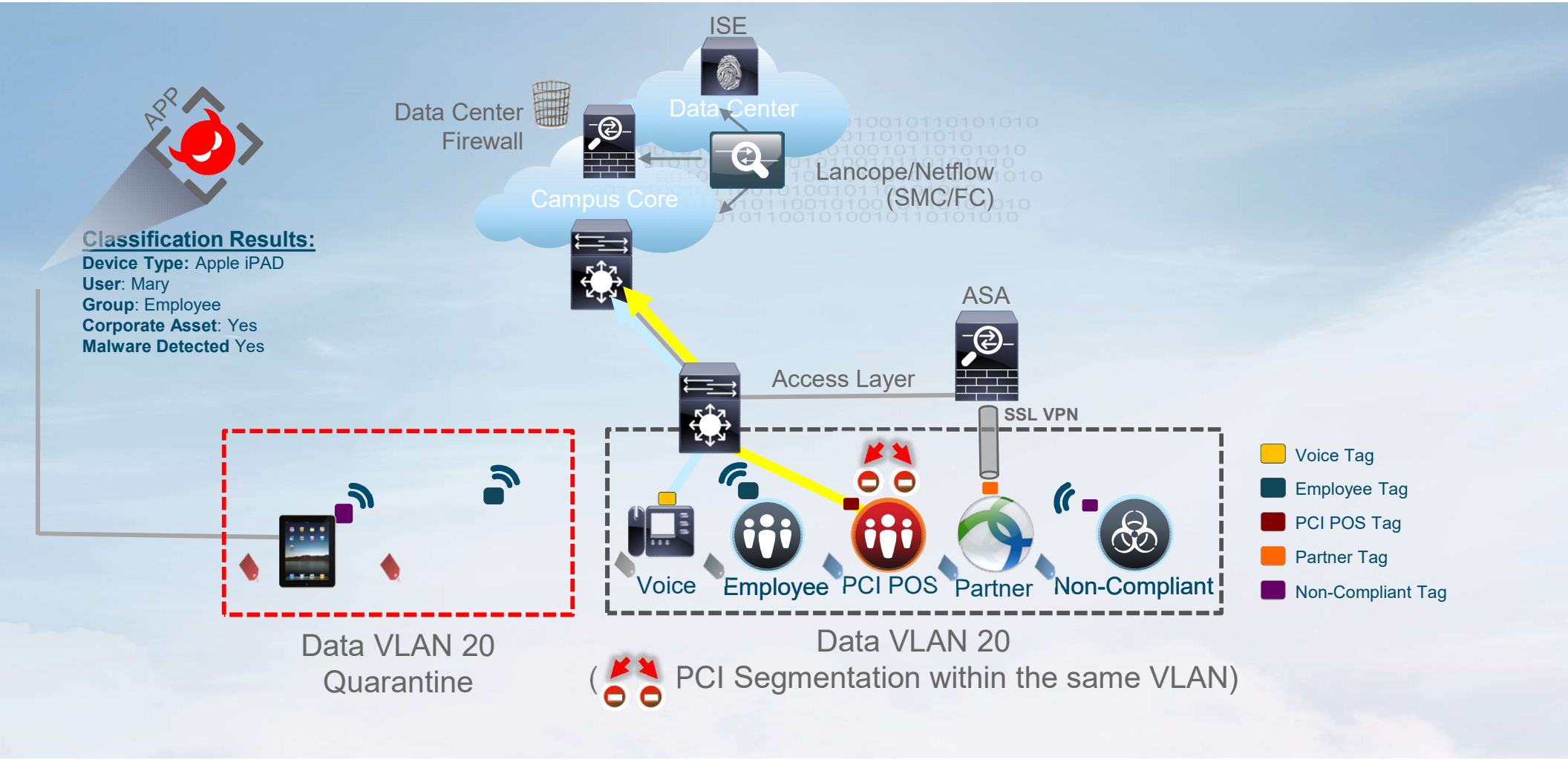
Simplifies Firewall Rule, ACL, VLAN Management

Prevents Lateral Movement of Potential Threats

Eliminates Costly Network Re-architecture



Cisco TrustSec Software-Defined Segmentation



Segmentation is Powerful Security Tool

2014 DATA BREACH INVESTIVATIONS REPORT

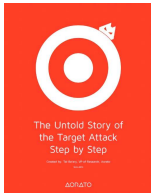
"Good network and role segmentation will do wonders for containing an incident."

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

"Effective network segmentation… reduces the extent to which an adversary can move across the network"

Australian Government
Department of Defence
Intelligence and Security

"Network segmentation… is one of the most effective controls an agency can implement to mitigate the second stage of a network intrusion, propagation or lateral movement"

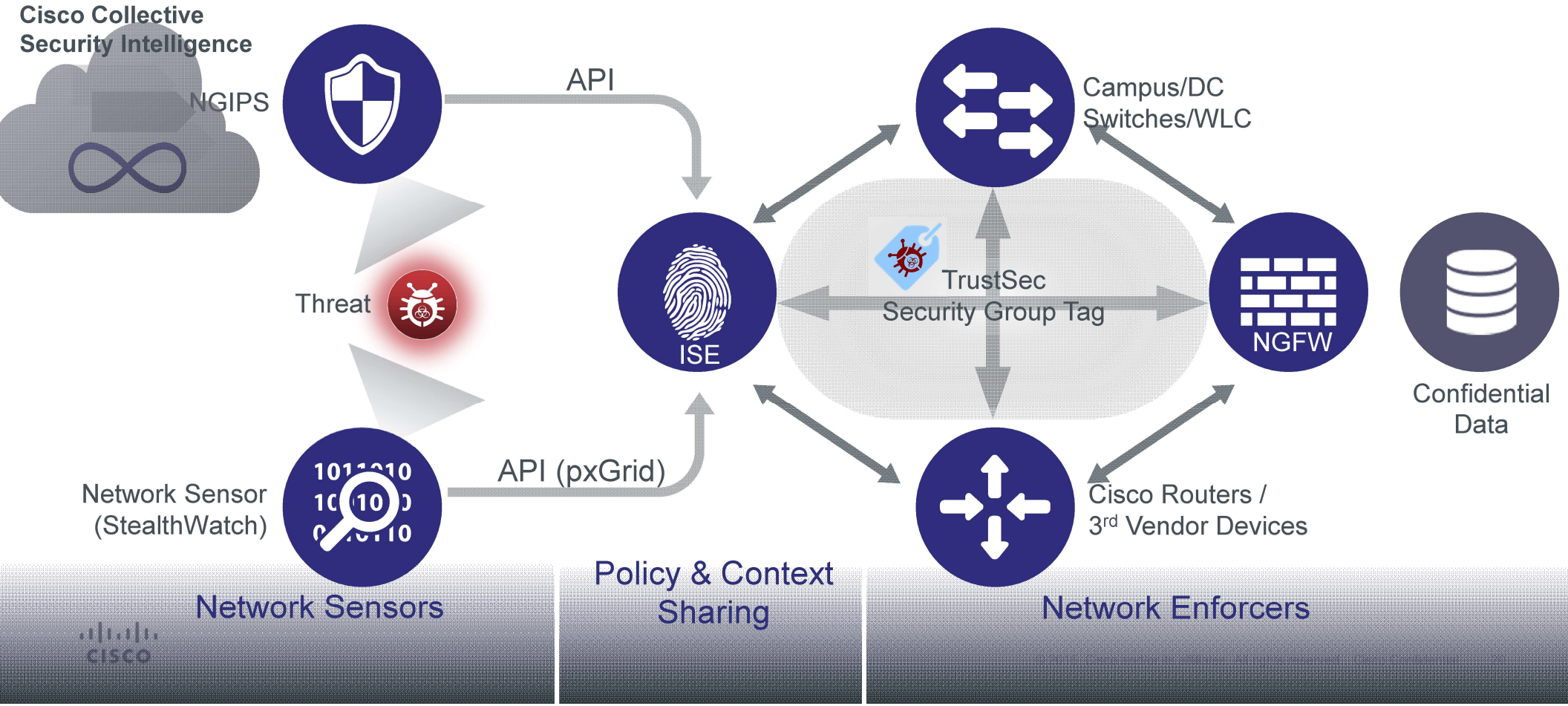


The Untold Story of the Target Attack Step by Step
Aortato Labs, August 2014

"Segregate networks, limit allowed protocols usage and limit users' excessive privileges."

Bringing It All Together

Architecting Network as a Sensor and Network as an Enforcer

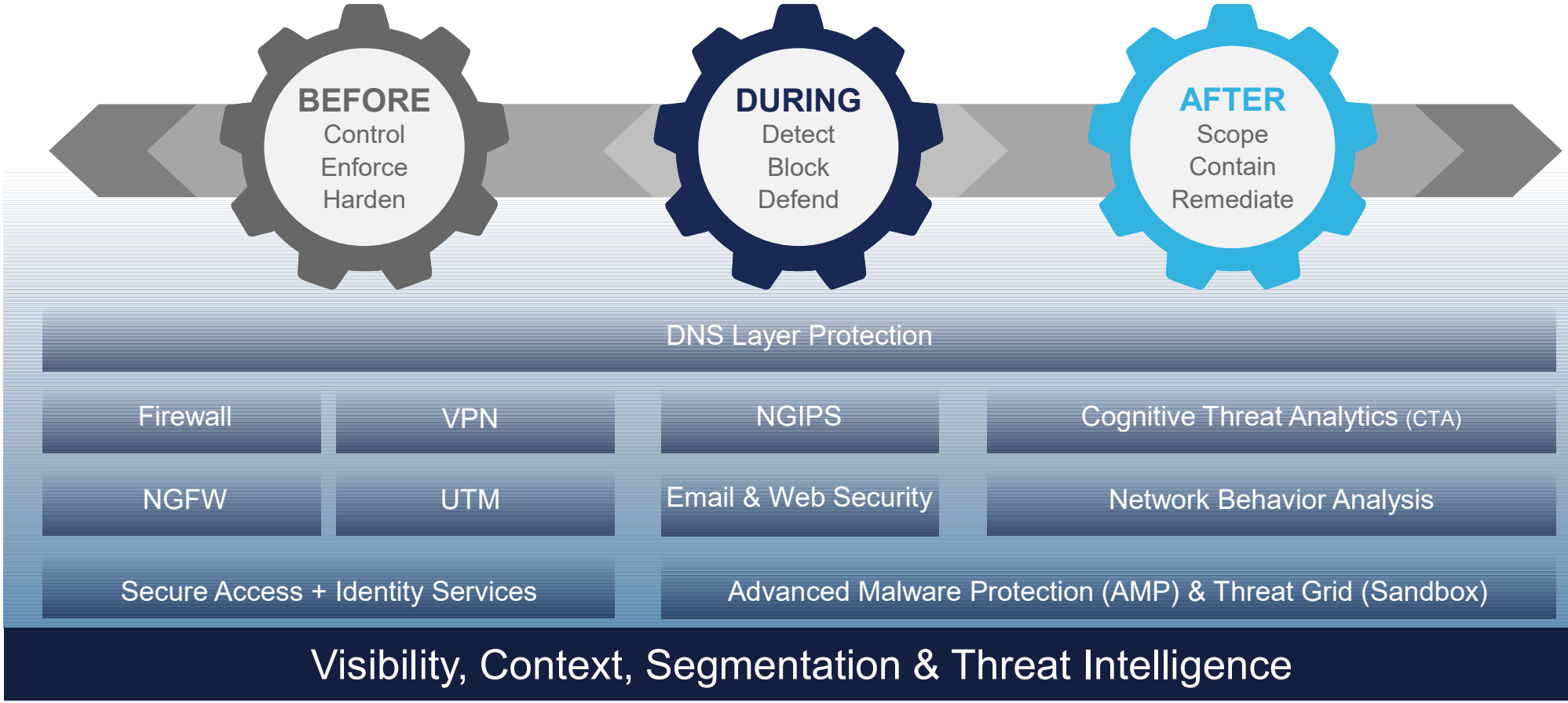


What Can Cisco NaaS & NaaE Offer Customers?

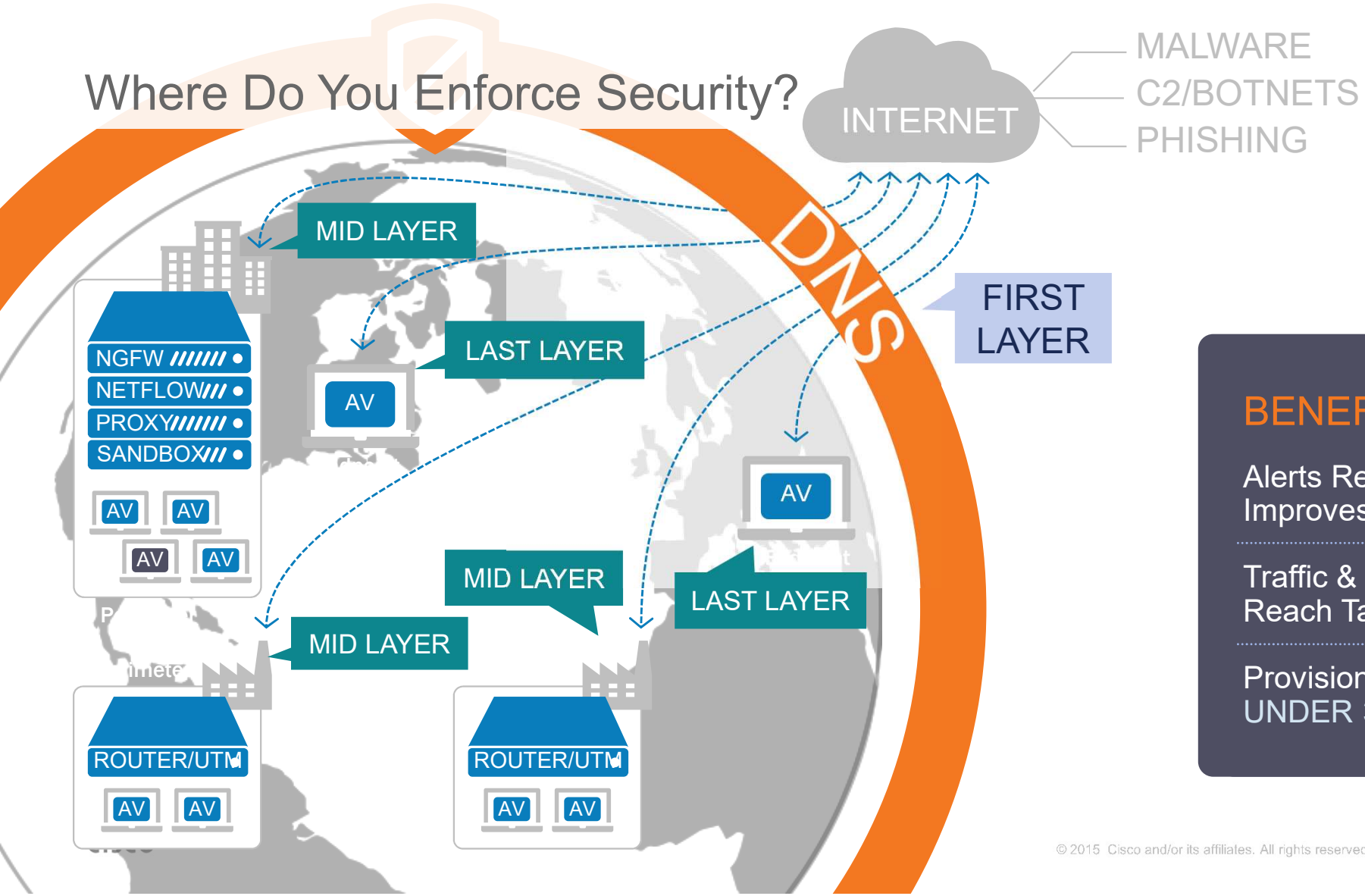
Unmatched Visibility	Consistent Control	Advanced Threat Protection	Complexity Reduction
			
Global Intelligence With the Right Context	Consistent Policies Across the Network and Data Center	Detects and Stops Advanced Threats	Fits and Adapts to Changing Business Models

First Layer of Defense: OpenDNS

Threat Centric model to cover the Entire Attack Continuum



Where Do You Enforce Security?



BENEFITS

Alerts Reduced 2-10x; Improves Your SIEM

Traffic & Payloads Never Reach Target

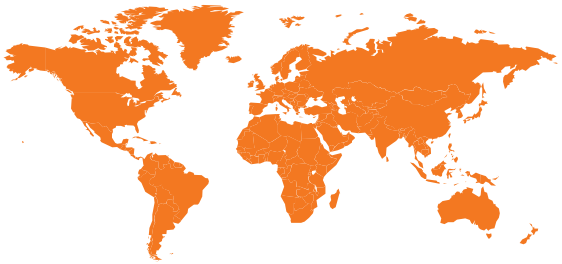
Provision Globally in UNDER 30 MINUTES

Why OpenDNS?

DNS Services Built for World's Largest Security Platform

GLOBAL NETWORK

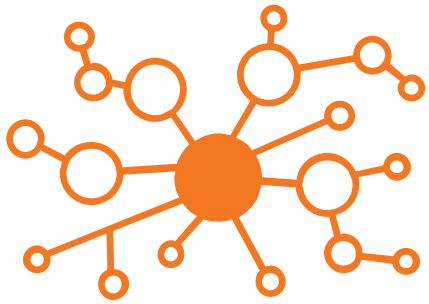
- 80B+ DNS requests/day
- 65M+ biz & home users
- 100% uptime
- Any port, protocol, app



+

UNIQUE ANALYTICS

- security research team
- automated classification
- BGP peer relationships
- 3D visualization engine



= **80M+**

malicious requests blocked/day

cisco

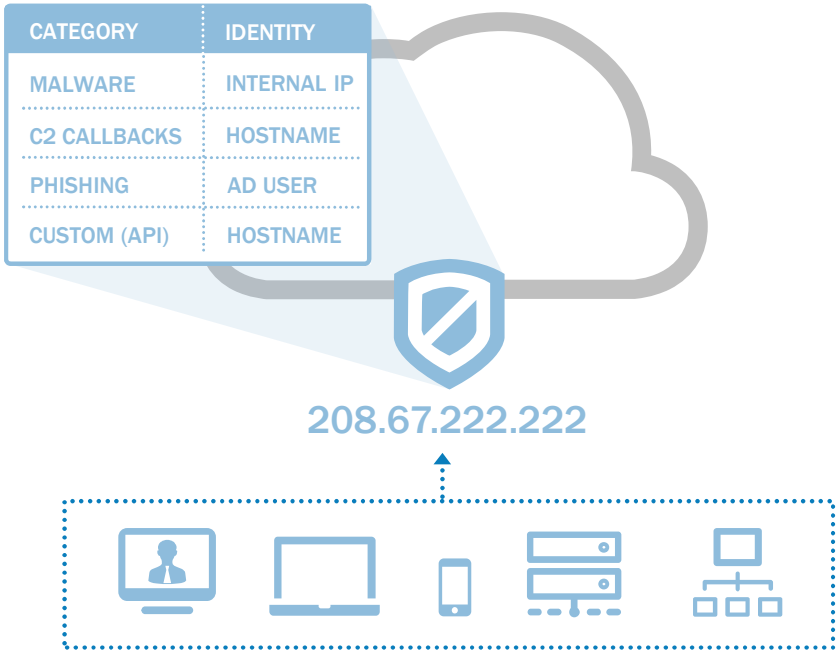
Nothing Kills Attacks Earlier Than DNS-Layer Network Security

DEPLOY IN MINUTES
POC IN <2 WEEKS

2-10X FEWER
ALERTS

INTEGRATE IN MINUTES
BLOCK IN SECONDS

UMBRELLA: The Fastest & Easiest Way To Prevent Threats Before They Reach You



BENEFITS

Simple to point DNS w/o technical or pro services

No hardware to install
No software to maintain

Provision globally in under 30 minutes

Infinitely scalable enforcement platform

A New Layer of Breach Protection

Threat Prevention
Not just threat detection

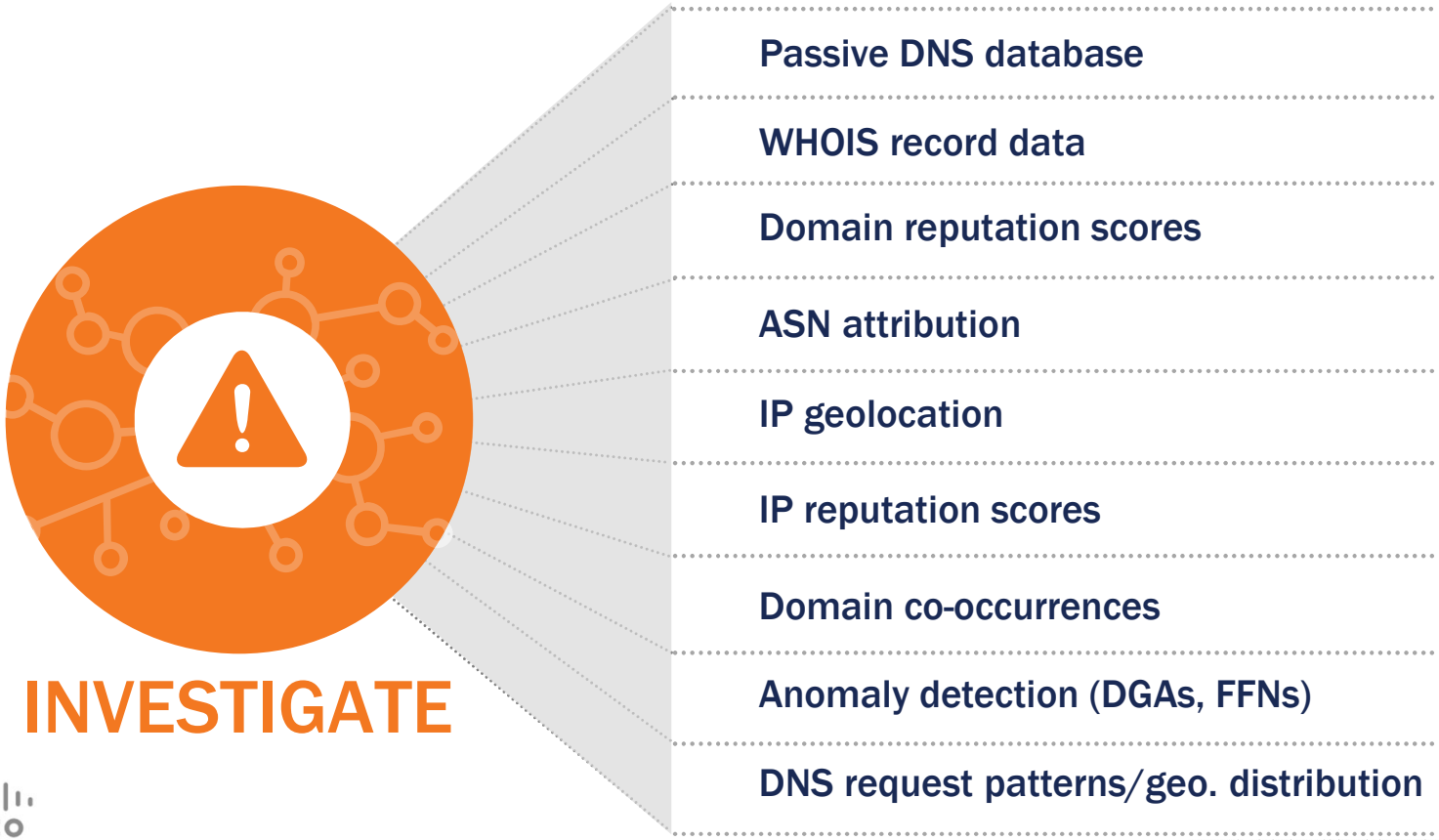
Protects On & Off Network
Not limited to devices forwarding traffic through on-prem appliances

Always Up to Date
No need for device to VPN back to an on-prem server for updates

Block by Domains, IPs & URLs for All Ports
Not just ports 80/443 or only IPs

Turn-Key & Custom API-Based Integrations
Does not require professional services to setup

A Single, Correlated Source of Information



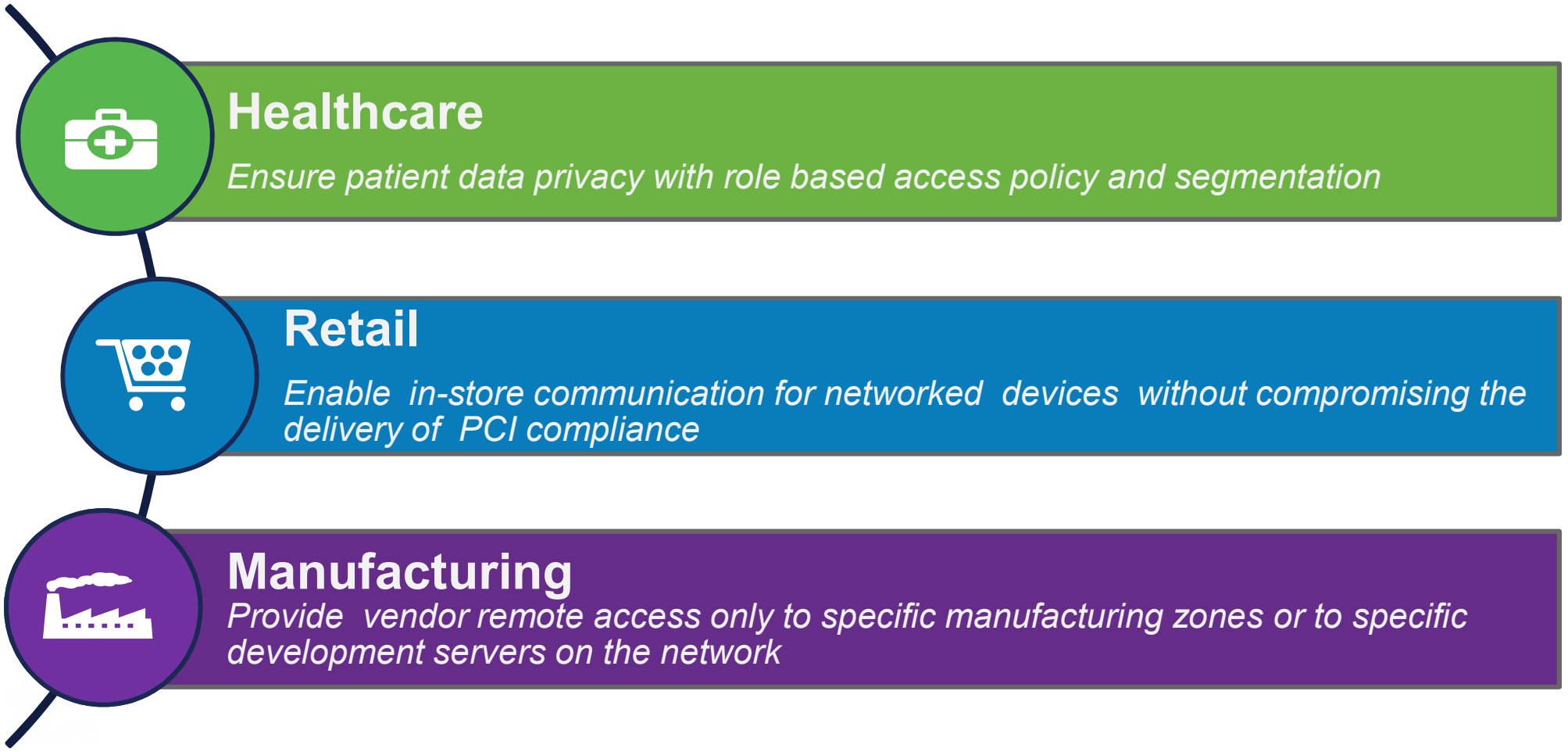
cisco

Use Our Global Intelligence To…

- Speed up investigations
- Stay ahead of attacks
- Prioritize investigations & response
- Enrich security systems with real-time data

Network as a Sensor/Network as an Enforcer Use Cases

Vertical Customer Use Cases



Customer Case Study - Network as a Sensor

Industry: Retail
Company: Large Known Global Retailer

Existing Environment:
- Large Cisco Switch & Router Footprint
- ASA & ISE

Customer Challenges:
- Limited visibility & intelligence across their highly-distributed retail footprint
- Lack of ability to correlate numerous data sets

Results:
- After deploying Cisco Netflow, Lancope Stealth Watch and Cisco ISE
- Gains Retail Point-of-Presence Visibility
- Deeper Understanding into Network Application Usage

Customer Case Study - Network as an Enforcer

Industry: Banking
Company: Large Known Global Bank

Existing Environment:
- Large Cisco Switch & Router Footprint

Customer Challenges:
- Visibility into the network and rogue devices
- Policy enforcement of user to data center policies
- Meeting compliance audits

Results:
- After deploying Lancope Stealth Watch Cisco ISE and Cisco TrustSec
- Gain Deep Visibility into Network Access and Devices
- Segment Network Access and Assets using Business Role Based Policies
- Accelerated time to Compliance Audits

TOMORROW starts here.