The Network as a Sensor

Securing the Enterprise Network

Complementing Advanced Malware Protection and Traditional Security

Brian Korn, Sr. Marketing Manager, Cisco
Chris Smithee, Director of Strategic Alliances, Lancope

Agenda

- Security Market Trends
  - You are Already Infected, Erosion of Trust
  - Attack Surface and Sophistication Increasing
  - Discovery of Breaches and Mitigation May Take Months
- The Threat Centric Security Model
  - Before, During, After An Attack
- The Role of the Network for Security
  - Network Complements Advanced Malware Protection and Perimeter Security
  - Network as a Sensor - You Can’t Protect What You Can’t See
  - Network as an Enforcer
  - Network as a Mitigation Accelerator

Global Enterprise Networks are Under Attack

Did You Know That You Are Already Infected?

Malicious Traffic is Visible on 100% of Corporate Networks*

Cisco 2014 Annual Security Report

*Companies connect to domains that host malicious files or services

Enterprise Attack Surface is Increasing

Sophisticated Threats Difficult to Detect

Slow and Complex Mitigation

* Ponemon Institute Study

Enterprise Attack Surface Is Increasing

Driven by Increase in Mobility, Cloud Services, and IoT

Mobile

3.3 Devices Per Knowledge Worker*

55% IP Traffic Mobile by 2017**

77B App Downloads in 2014***

* Cisco IBSG, ** Cisco 2013 VNI, *** IDC

Cloud

545 Cloud Apps Per Organization*

3X Cloud Traffic Growth by 2017**

44% Annual Cloud Workload Growth***

* Skyhigh Networks Industry Report, ** Cisco Global Cloud Index, *** Cisco VNI Global Mobile Data Traffic Forecast,

IoT

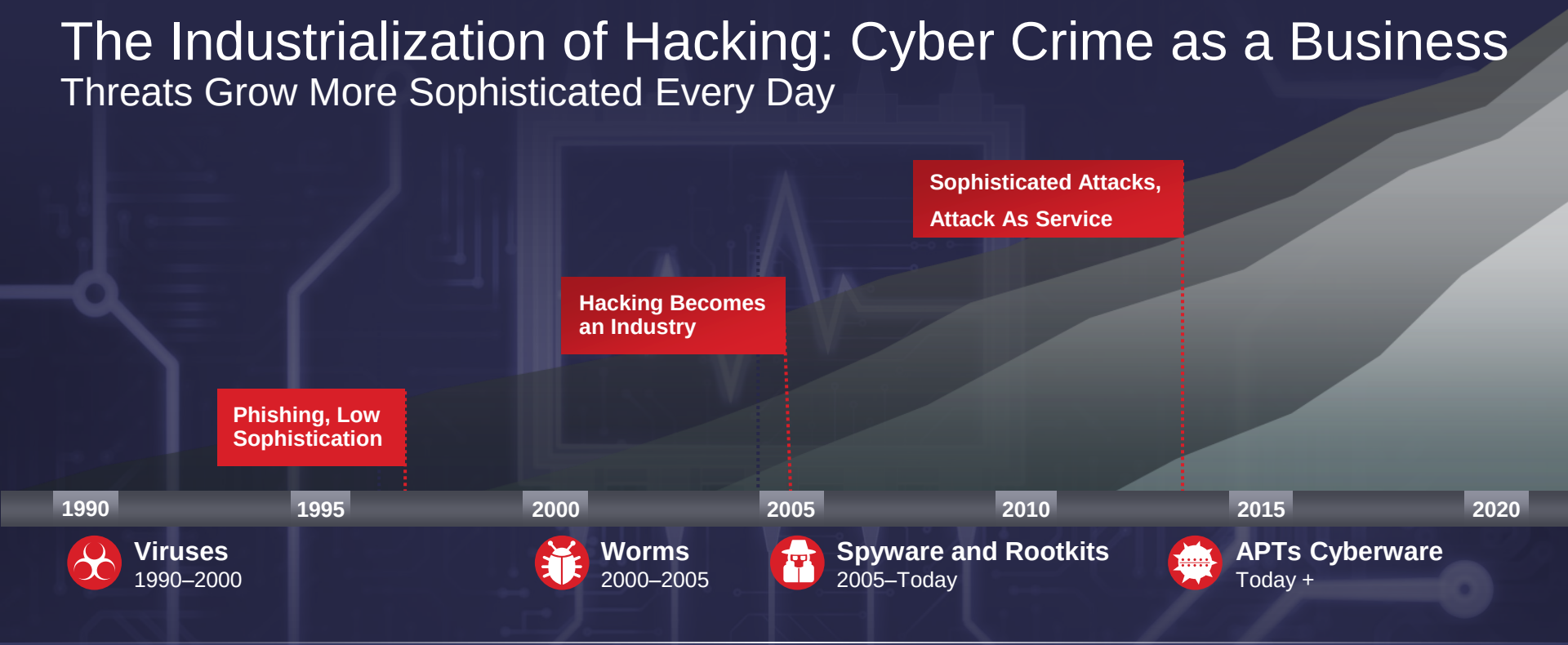
50B Connected "Smart Objects" by 2020*

36X Growth in M2M IP Traffic 2013–18**

* Cisco IBSG, ** Cisco VNI: Global Mobile Data Traffic Forecast 2013-2018

The Industrialization of Hacking: Cyber Crime as a Business

Threats Grow More Sophisticated Every Day



Criminals Know More About Your Network Than You Do

Initial Malware May Remain Dormant For Months to Learn Vulnerabilities and Network
Custom Malware Developed to Attack After Learning Your Vulnerabilities

How Industrial Hackers Monetize the Opportunity

Social Security $1

Medical Record >$50

Credit Card Data $0.25−$60

DDoS as a Service ~$7/hour

$

Bank Account Info >$1000
depending on account type and balance

Global Cybercrime Market: $450B-$1T

Mobile Malware $150

Spam $50/500K emails

Malware Development $2500
(commercial malware)

Exploits $100k-$300K

Facebook Account $1 for an account with 15 friends

Welcome to the Hackers' Economy

Source: CNBC

Discovery of Breaches Takes a Long Time

Attackers are Fast, Defenders are Slow

60%
of data is stolen
in **hours**

54%
of breaches
remain undiscovered
for **months**

100%
of companies connect
to domains that host
malicious files
or services

Malicious Breaches take
80 Days to Discover
123 Days to Resolve on Average

Ponemon Institute Study

Threat Mitigation and Remediation Takes Even Longer

An Erosion of Trust

Nothing Should be Trusted – Apps, Certificates, Cloud, Devices, Users…

“Treat Every User as Hostile.”

Stolen Identity, Malicious Intent

CIO of a Global Investment Banking, Securities, Investment Management Firm

“Treat Enterprise as Untrusted.”

Senior Executive of a Global Internet Search Firm

“Network Security is Critical”

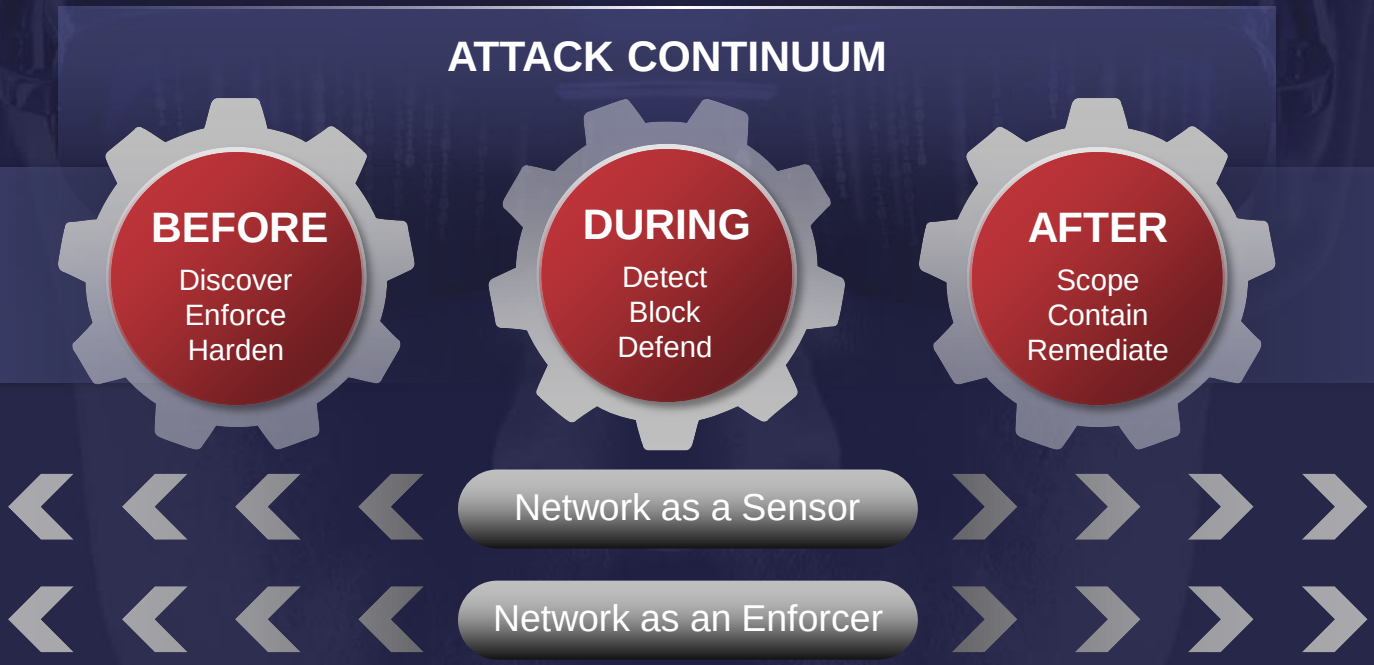
Network has the Visibility of
Devices, Users, Location, and Applications

Art of Network Security
Strategic Advice

Unite the Forces

Advanced Malware Protection
Threat Centric Security
Network as a Sensor, Enforcer, and Mitigation Accelerator

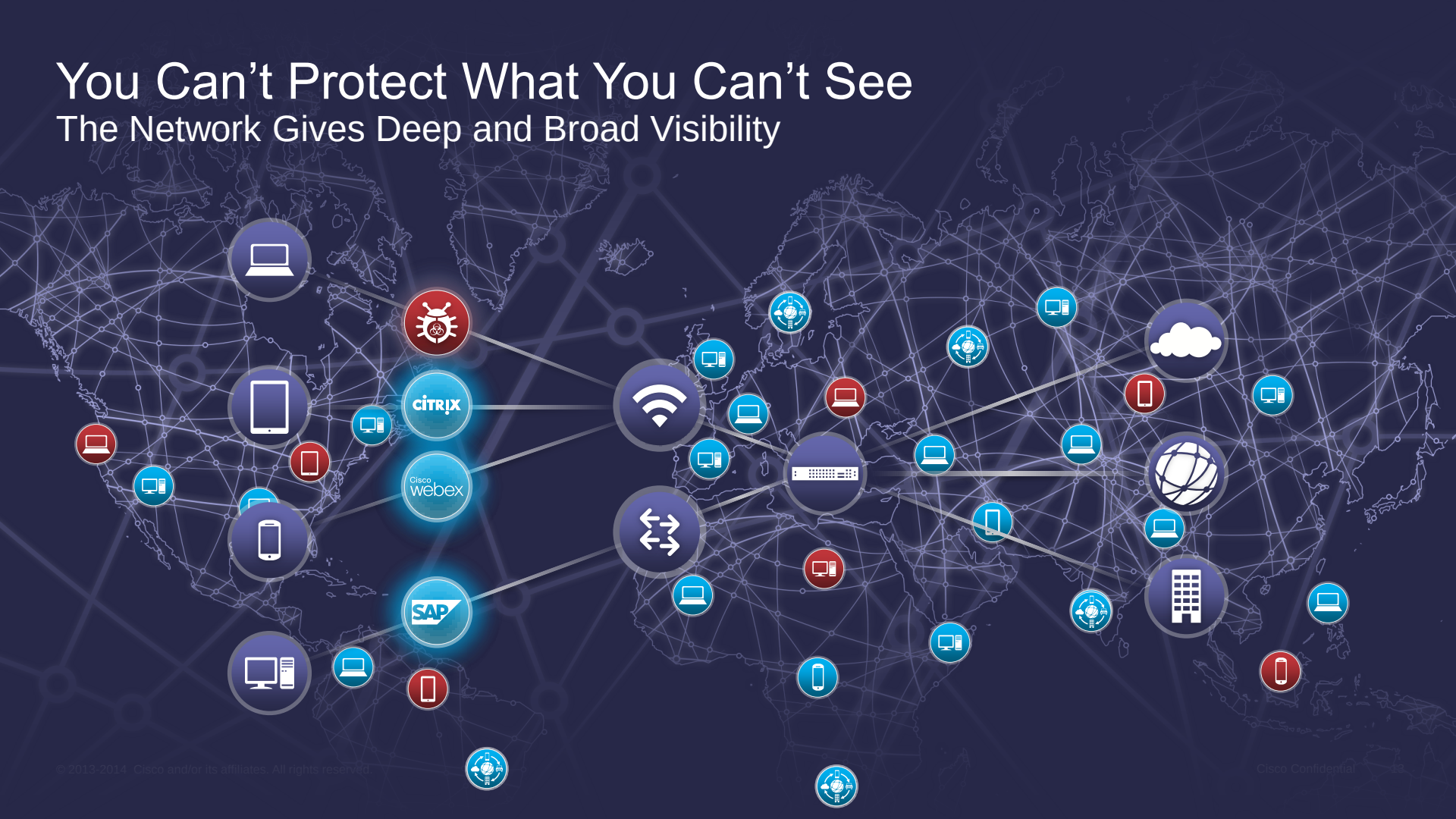
The Threat Centric Security Model



Visibility & Defense Across the Entire Attack Continuum

You Can’t Protect What You Can’t See

The Network Gives Deep and Broad Visibility



What Can the Network Do for You?

Network as Sensor

Detect Anomalous Traffic Flows, Malware

e.g. Communication with Malicious Hosts, Internal Malware Propagation, Data Exfiltration

Detect App Usage, User Access Policy Violations

e.g. Contractor Accessing Financial Data

Detect Rogue Devices, APs and More

e.g. Maintenance Contractor Connecting an Unauthorized AP in Bank Branch to Breach

NetFlow – The Heart of Network as a Sensor

Path to Self Learning Networks

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 are Attack Signatures

Lancope StealthWatch Provides Detailed Visibility

Drilling into a single flow provides a plethora of information

ISE: Network-Wide Policy Enforcement

Unified Policies Across the Distributed Enterprise

- ✓ Guest Access
- ✓ Profiling
- ✓ Posture

WHO | WHAT | WHERE | WHEN | HOW

CONTEXT

Security Camera G/W
Agentless Asset
Chicago Branch

Vicky Sanchez
Employee, Marketing
Wireline
3 p.m.

Francois Didier
Consultant
HQ - Strategy
Remote Access
6 p.m.

Frank Lee
Guest
Wireless
9 a.m.

Personal iPad
Employee Owned
Wireless HQ

IDENTITY

- ✓ 802.1X
- ✓ MAB
- ✓ WebAuth

CISCO SWITCHES, ROUTERS, WIRELESS ACCESS POINTS

Identity (802.1X)-Enabled Network

Network as a Sensor

More Intelligence, Richer Context – NetFlow, ISE & Lancope Integration

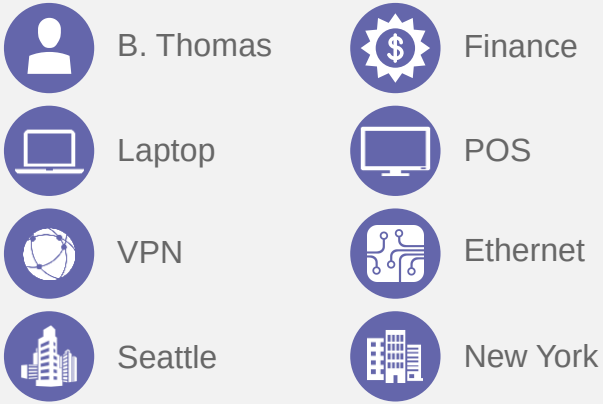
Before

Host 1.2.3.4 Scanning Ports of Host 3.3.3.3

- Not Intuitive
- Complex
- Long Time to Identity
  User Device, Location

Now

Host 1.2.3.4 Scanning Ports of Host 3.3.3.3



Identity Malicious Traffic Faster with More Context
Enhanced Visibility – User, Location, Device

StealthWatch Use Cases

Context-Aware Visibility

- Network, application and user activity
- East-West traffic monitoring

Threat Detection

- Advanced Persistent Threats
- Insider Threat
- DDoS
- Data Exfiltration

Incident Response

- In-depth, flow-based forensic analysis of suspicious incidents
- Scalable repository of security information

Network Diagnostics

- Application Awareness
- Capacity Planning
- Performance Monitoring
- Troubleshooting

User Monitoring

- Cisco ISE
- Monitor privileged access
- Policy enforcement

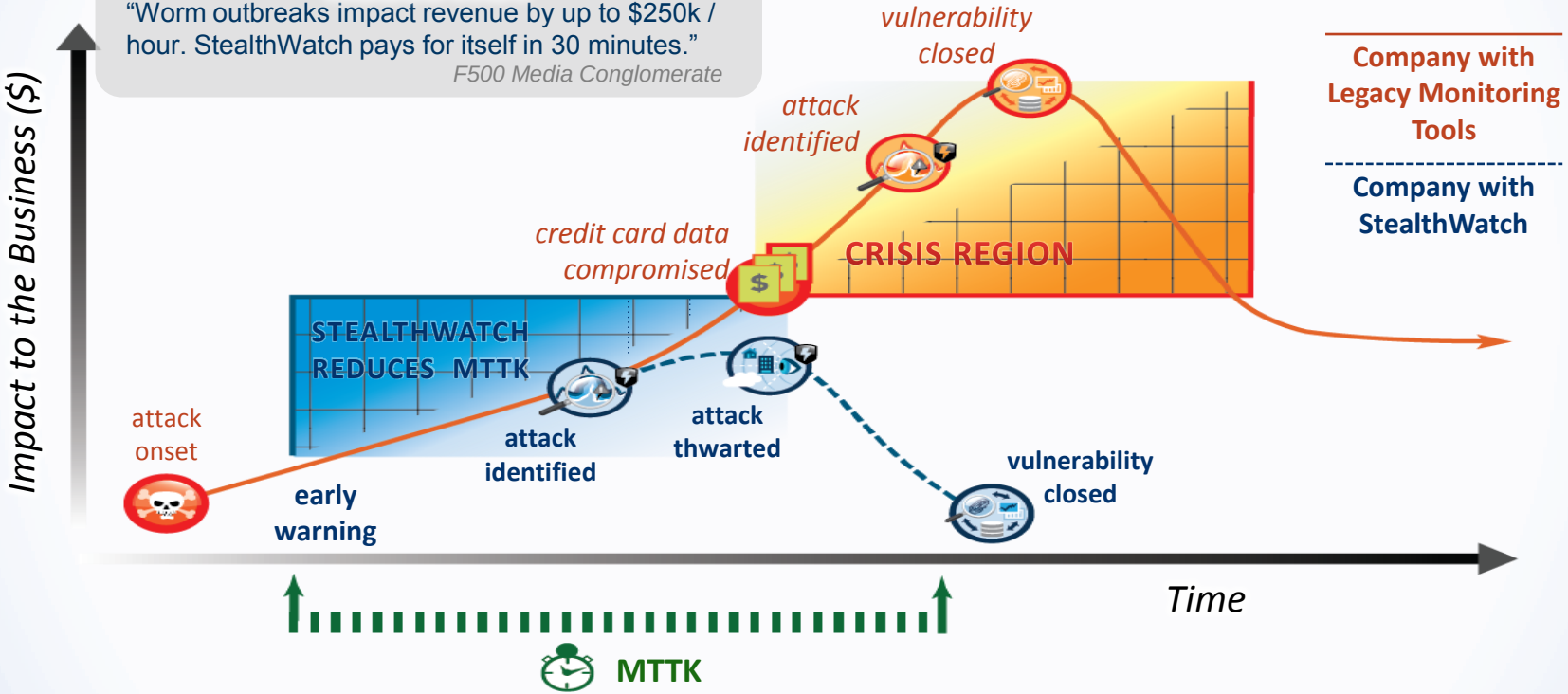
Lancope

Stop Problems Before They Become Crises

259% ROI

"Worm outbreaks impact revenue by up to $250k / hour. StealthWatch pays for itself in 30 minutes."

F500 Media Conglomerate



~70% of Incident Response is spent on MTTK

Lancope

Art of Network Security

Strategic Advice

Know Your Normal

Network as a Sensor
Traffic, Flows, Apps, Devices, Users

Network as an Enforcer

What Can the Network Do for You?

Network as Enforcer

Segment the Network to Contain the Attack

TrustSec - Secure Group Tagging, VRF, ISE and More

Encrypt the Traffic to Protect the Data in Motion

MACsec for Wired, DTLS for Wireless, IPSec/SSL for WAN and More

Secure The Branch for Direct Internet Access

IWAN, Cloud Web Security and More

Art of Network Security
Strategic Advice

Divide and Defend

Segment the Network to Contain the Attack
TrustSec, ISE, VLAN/VRF/EVN, ACLs

Segment the Network and Enforce Policy to Contain the Attack

Network as an Enforcer

Segment Network

To Contain the Attack

Role-Based, Topology and Access-Independent Access Control (TrustSec/SGT, ISE)

Network Segmentation (VLAN, TrustSec/SGT, VRF/EVN)

Access Control

For Granular and Consistent Policy

User Access Control based on Device, Location, Network Type, Time, and More (ISE)

Physical and Virtual Port-Level Permit and Denial (Access Control Lists)

Consistent Policy Across Wired/Wireless/Remote Access (ISE, Unified Access Switches)

Cisco TrustSec

Identity-Based Software Defined Segmentation

Desired Policy

- Who can talk to whom
- Who can access protected assets
- How systems can talk to other systems

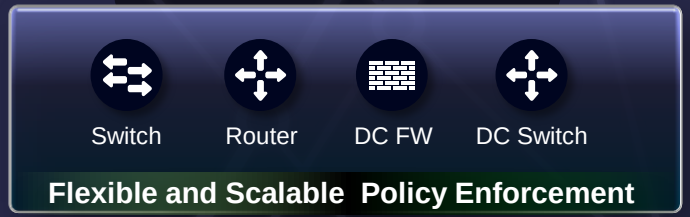
Protected Assets

Source	Production Servers	Development Servers	Internet Access
Employee (managed asset)	PERMIT	DENY	PERMIT
Employee (Registered BYOD)	PERMIT	DENY	PERMIT
Employee (Unknown BYOD)	DENY	DENY	PERMIT
ENG VDI System	DENY	PERMIT	PERMIT

Simplified Access Management

Accelerated Security Operations

Consistent Policy Anywhere

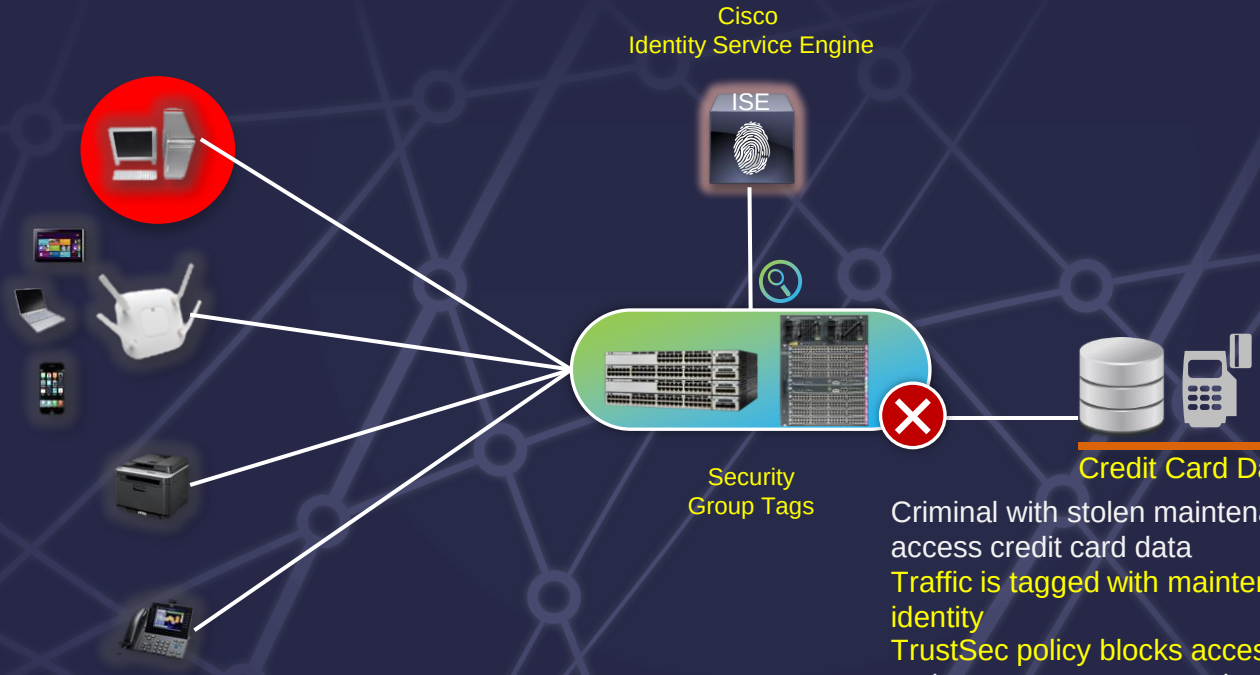


Block Stolen Credentials from Accessing Credit Card Data

TrustSec Identity-Based Segmentation to Contain the Attack

Detect

Enforce



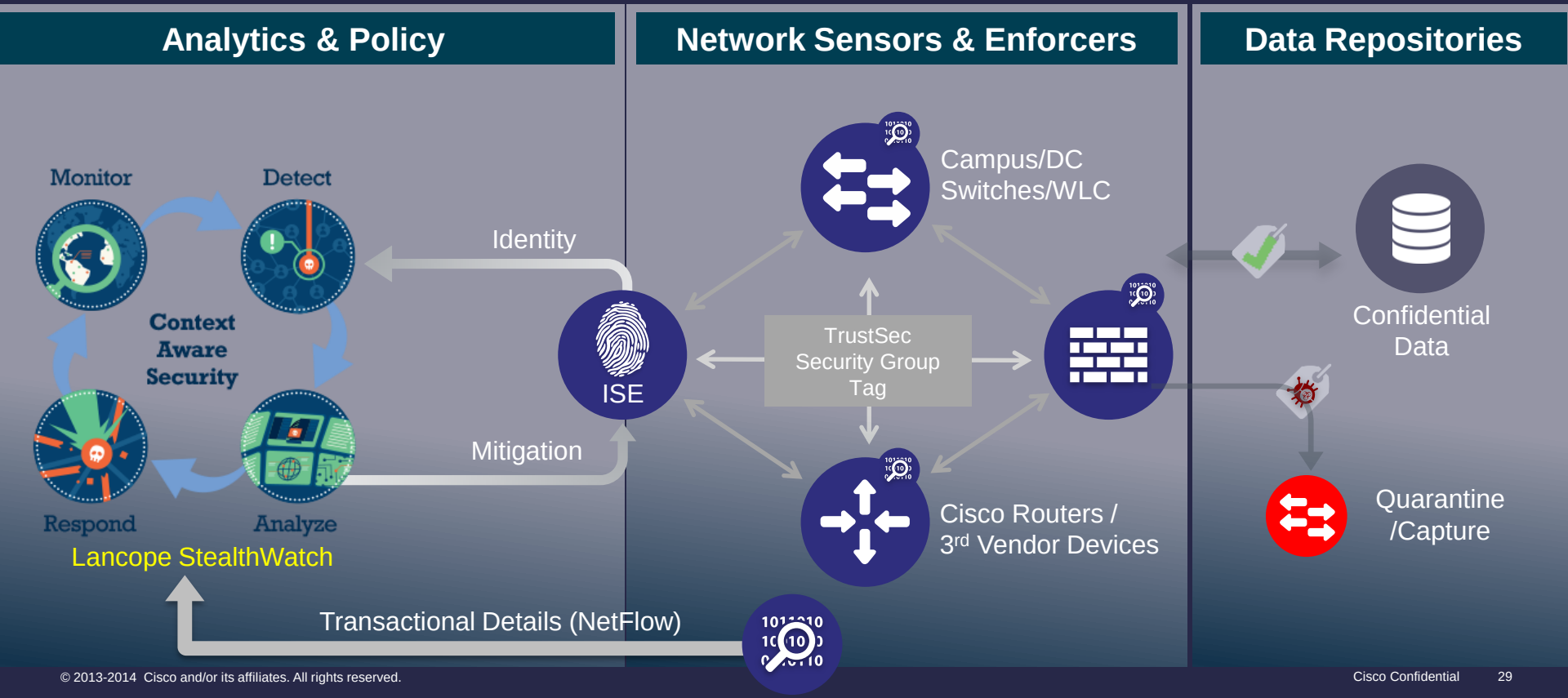
Criminal with stolen maintenance contractor identity tries to access credit card data

Traffic is tagged with maintenance contractor user group identity

TrustSec policy blocks access to credit card data due to maintenance group tag mismatch with financial group tag

ISE enforces policy across Wired, Wireless, and VPN

Cisco TrustSec with Lancope StealthWatch



Art of Network Security
Strategic Advice

Enable Built-In Network Defenses

You Have Already Invested in Your Network
Activate TrustSec, NetFlow, Encryption, and More.

Network as a Mitigation Accelerator

What Can the Network Do for You?

Network as a Mitigation Accelerator

Decrease Time to Remediation

e.g. SourceFire Integration for Network-Wide Rapid Threat Detection and Mitigation

Automate Configuration and Provisioning

e.g. ACL, QoS, and Secure Branch Automation

Enable Open, Programmable Network Abstraction

e.g. RESTful API Integration, CLI Hardware Compatibility

Attackers are Fast, Defenders are Slow

Today's Security Model - Complex, Not Fast Enough

Box by Box
Manual Configuration

Discovery of Breaches Takes a Long Time

Threat Mitigation Takes a Long Time Too

Cisco Vision: Network as Security Sensor and Enforcer, Accelerated by ACI

Policy-Based Security at Scale
Open & Automated
Enabled By APIC-EM

Current direction of roadmap

Art of Network Security
Strategic Advice

Unite the Forces

Advanced Malware Protection
Threat Centric Security
Network as a Sensor, Enforcer, and Mitigation Accelerator

Thank you.