Understanding Cisco’s Security Focus And Its Integrated Architectural Approach

John McCurdy
Vice President, Americas, Global Security Sales Organization (GSSO)
June 2016
A Familiar View
Another Point Of View
Rapid Digital Disruption on a Massive Scale

$19 Trillion Opportunity

15B Devices Today

500B In 2030

$19 Trillion Opportunity
Digital Disruption Drives the Hacker Economy

...Creating an ever-evolving, dynamic threat landscape
The Silver Bullet Does Not Exist…

Cisco focuses on the totality of defending against threats.
“If you can truly accomplish what you just described (contextual based alerts), you will change the security industry.”

- CISO, Fortune 500 Financial at Sourcefire Seminar 2003
You Can't Protect What You Can't See

Collective Security Intelligence

Threat Intelligence

Research Response

Solutions must be security driven.
Only a Cisco Network Sees Everything
A Threat-Centric Security Model

ATTACK CONTINUUM

BEFORE
Discover Enforce Harden

DURING
Detect Block Defend

AFTER
Scope Contain Remediate

Network Endpoint Mobile Virtual Cloud

Point-in-Time Continuous
Cisco’s Differentiating Approach

Integrated Threat Defense
“Network security architects should accept the reality that, in 2016, it is unreasonable to expect that they can build perimeter defenses that will block every attack and prevent every security breach…

Instead, they need to adopt new products and/or services that will enable the network to be an integral part of a strategy that focuses on detecting and responding to security incidents.”
“I would settle for 80% of the functionality of my best-in-breed security products, if I could just have security solutions that were integrated and worked together.”

- CISO, Fortune 500 Financial
"Most of the organizations you've read about getting hacked had all the modern defenses. They had the sandboxes and NGFWs, AV and IPS and they still got hacked despite detecting the actual attacks! The complexity of operating all of this infrastructure is so high that almost nobody can deal with it."

Marty Roesch Keynote @ RSA 2015
VP & Chief Architect, Cisco Security Business Group
Goal for Effective Security
Closing the Effectiveness Gap

Integration

Consolidation

Automation
“We are a huge Cisco shop, but we haven’t been using Cisco Security.”

- CISO, Fortune 500 Energy 2013

Then how are you doing retrospective security...changing your mind about past files you deemed safe, but later learned were actually malicious?
Retrospective Security

Always Watching… Never Forgets… Turns Back Time

Continuous Analysis - Retrospective detection of malware beyond event horizon

Trajectory – Determine scope by tracking malware in motion and activity
  - File Trajectory – Visibility across organization, centering on a given file
  - Device Trajectory – Deep visibility into file activity on a single system

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential.
Advanced Malware Protection: Exponential Growth

![Graph showing exponential growth in advanced threat protection customers over quarters FY14 to FY16, with Cisco AMP leading and Vendor A and Vendor B lagging behind. The graph peaks at 10,800+ total customers by Q2 FY16.](image-url)
The Right Question to Ask Our Customers:

Would you do security differently if you KNEW you were going to be compromised?
Incident response teams are being put in place, and 2 year project plans are being compressed into 8 months.

How quickly can they scope, contain and remediate?

The hot topic facing IT Security professionals is resiliency.
“I hear you and it all sounds great, but will Cisco continue on this path?”

- CISO, Fortune 500 Retailer
Security is Cisco’s #1 priority. We are going big and making strategic investments to become our customers’ and partners’ most trusted security advisor.

John Chambers
April 2015
Key Milestones for Cisco Security

- **2013**
  - Cognitive Acquired
  - RSAC: AMP Everywhere; OpenAppID
  - ThreatGRID acquired

- **2014**
  - Black Hat 2014: Talos
  - Cisco ASA w/ FirePOWER Services
  - ACI + FirePOWER Services

- **2015**
  - Global Security Sales Organization
  - Integrated Threat Defense Vision
  - Security Everywhere
  - ACI + FirePOWER Services
  - Neohapsis Acquired
  - OpenDNS Acquired
  - AMP Everywhere w/Threat Grid Incident Response Service
  - Cisco ASA w/ FirePOWER Services for Mid-Size and Branch environments

- **2016**
  - Security Everywhere Extended
  - OpenDNS/Threat Grid Integrated
  - Portcullis acquired
  - Lancope Acquired
  - Firepower NGFW and Security Advisory Service for Segmentation unveiled
Strategic Imperatives

Visibility-Driven
Network-Integrated, Broad Sensor Base, Context and Automation

Threat-Focused
Continuous Advanced Threat Protection, Cloud-Based Security Intelligence

Platform-Based
Agile and Open Platforms, Built for Scale, Consistent Control, Management

Network
Endpoint
Mobile
Virtual
Cloud
A Security Architecture Requires

Integration

Consolidation

Automation
Integrated Threat Defense Architecture

Faster Time to Detection, Faster Time to Remediation
INTELLIGENCE

Who is doing the homework?  
Who is your organization partnered with?

Intelligence is the FUEL behind security solutions.

CISCO’S TALOS Team
MULTI-TIERED DEFENSE

Talos is divided into 5 departments
Decryption tool available for TeslaCrypt ransomware that targets games

Lucian Constantin
IDG News Service  Apr 28, 2015 3:15 AM

Some users whose computers have been infected with TeslaCrypt might be in luck: security researchers from a tool to recover their encrypted files.

TeslaCrypt appeared earlier this year and masqueraded as CryptoLocker ransomware. However, its authors see the tool as particular.

Level 3, Cisco Team to Squash Major Botnet

Level 3 Communications is publicly discussing a collaborative effort to block a major botnet/DoS source, in hopes it can lead to more similar efforts. One goal is to encourage the industry, including major ISPs, to make it harder to try to shut down such attackers, not just identify, major cyber threat sources.

The collaborative effort involved Level 3 Communications Inc. (Nasdaq: LCSO) and Cisco Systems Inc. (Nasdaq: CSCO)’s Threat Research Labs and Cisco Systems Inc. (Nasdaq: CSCO)’s

Angler Take Down

Cisco Takes Down $60 Million Worldwide Hacker Operation

By Jai Cozza / NewsFactor Network

1. Cisco, Threat Research Labs
2. Find and Block a Major Botnet
3. Targeted an Internet-wide scanning and DDoS botnet that Cisco
4. SSHPsychos.Cisco had noticed that the Talos honeycomb -- the device
5. a key to the attackers or intruders -- were malicious traffic from this one attacker than from all others combining
6. network data confirmed the size of the attack, which at times accounted
7. of 38% of total Internet SSH traffic. SSH stands for Secure Shell
encrypted network protocol for access to remote machines.

SSHPsychos was using identified Linux malware and toolkit for DD
do and its brute force approach to gaining authentication. It essentially
A Threat-Centric Security Model

ATTACK CONTINUUM

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Network
Endpoint
Mobile
Virtual
Cloud

Point-in-Time
Continuous
Covering the Entire Attack Continuum

### Attack Continuum

<table>
<thead>
<tr>
<th>Before</th>
<th>During</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover</td>
<td>Detect</td>
<td>Scope</td>
</tr>
<tr>
<td>Enforce</td>
<td>Block</td>
<td>Contain</td>
</tr>
<tr>
<td>Harden</td>
<td>Defend</td>
<td>Remediate</td>
</tr>
</tbody>
</table>

### Security Services

- **Firewall**
- **VPN**
- **NGIPS**
- **Advanced Malware Protection**
- **NGFW**
- **UTM**
- **Web Security**
- **Malware Sandboxing**
- **Secure Access + Identity Services**
- **Email Security**
- **Network Behavior Analysis**
Illustration:
Force Multiplier
Report Identifies Ransomware Biggest Cost to Be Business Downtime

Big-Name Sites Hit by Rash of Malicious Ads Spreading Crypto Ransomware

New malvertising campaign may have exposed tens of thousands in the past 24 hours.

Ransomware: Coming to a Business Near You

Ransomware Is Targeting US Companies of All Sizes

A Top Cybersecurity Firm Says Ransomware Threats Expected to Grow

FBI Says Ransomware Attacks Are Getting Worse
User Clicks a Link or Malvertising → Malicious Code Launches → Malicious Infrastructure → Ransomware Payload
User Downloads Malicious Email Attachment

OR

Ransomware Payload
YOUR FILES ARE ENCRYPTED!
How Cisco Protects Customers

- **OpenDNS**: blocks the request
- **Next-Gen Firewall**: blocks the connection
- **Web Security w/AMP**: blocks the file
- **Lancope**: detects the activity
- **AMP for Endpoint**: blocks the file & communication back to home
Email Security w/AMP blocks the file

AMP for Endpoint blocks the file & communication back to home
Architectural Force Multiplier
Cisco Protects from the Network to the Endpoint to the Cloud

**OpenDNS**
Security from the cloud
Blocks 95% of threats before they cause damage

**AMP**
See a threat once, block it everywhere
Most effective solution for known and emerging advanced threats

**Next-Gen Firewall**
Prioritizes threats
Automates response
Improved malware protection
Fully integrated management

**Lancope / StealthWatch**
Alerts attempted communication with an infected host
Prevents infected host from communication within the network
Uses Network as a Sensor to contain and minimize threats
Rapid Threat Containment in Action

Automatically Defend Against Threats with FMC and ISE

1. Corporate user downloads file, not knowing it’s actually malicious
2. Cisco security sensors scan the user activity and downloaded file. FMC aggregates and correlates sensor data
3. FMC detects flagrantly suspicious file and alerts ISE. ISE then changes the user’s/device’s access policy to suspicious
4. Based on the new policy, network enforcers automatically restrict access
5. Device is quarantined for remediation or mitigation—access is denied per security policy
Gain Greater Visibility and Control
Rapid Threat Containment now offering Threat-centric NAC

What’s new for ISE 2.1?
ISE now incorporates vulnerability assessments from Qualys and threat incident intelligence from Talos and AMP, helping you ensure your policies account for the latest vulnerabilities and threats.

Benefits
- Deeper visibility that extends to all endpoints on the network
- Expanded control driven by threat intelligence and vulnerability assessment data
- Faster response with automated, real-time policy updates based on vulnerability data

Capabilities
- Author intelligent policies informed with new threat and vulnerability data
- Eliminate unknowns and ensure device compliance
- Take immediate action on high-priority issues
- Gain awareness when a vulnerability score changes or a threat is detected, and adjust network privileges
- Automate containment of vulnerable endpoints based on vulnerability score

Who
Where
What
How
When
Compliant
Threat
Vulnerability
Threat Centric NAC

Correlating Threat and Vulnerability Information to reduce Time to Remediate with ISE Network Fabric Visibility and Control

- Discover Vulnerable Embedded IOT Devices
- Automated containment of vulnerable endpoints based on CVE Score
- Immediate action on prioritized vulnerability to maximize SOC resources
“Based on our (Breach Detection Systems) reports, Advanced Malware Protection from Cisco should be on everyone’s short list.”

“Cisco is disrupting the advanced threat defense industry.”

“2014 Vendor Rating for Security: Positive”

“So do any network security vendors understand data center and what’s needed to accommodate network security? Cisco certainly does.”

“… AMP will be one of the most beneficial aspects of the [Sourcefire] acquisition.”

“The AMP products will provide deeper capability to Cisco’s role in providing secure services for the Internet of Everything (IoE).”
Security Services (by Cisco & its Partners)

Portfolio

FY15 (17?) Security Services

Advisory
- Custom Threat Intelligence
- Vertical Security Assessments

Integration
- Integration Services
- Security Optimization Services

Managed
- Managed Threat Defense
- Secure Plant Operations
Security Leads to Higher Profitability
Leading with security provides upsell, cross sell and migration capabilities throughout the network

Most Profitable Partners* Sell Security Solutions

Expanded deal size

Increased services, revenues and margins

Increase cross architecture sales

Recurring revenue, Incumbency Protection

Business Outcome Selling

*June 2015 Cisco Sponsored Profitability Study done by Global Touch Inc
Differentiated Threat Defense

Advanced, Automated Malware Detection

Contextual Visibility to Understand and Contain Threats Faster

Continually Updated Threat Intelligence

Pervasive Network Enforcement

Your Cisco Network as Security Sensor and Enforcer
TOMORROW starts here.