Cisco Security Strategy Update
Integrated Threat Defense

Oct 28, 2015
Breaches are the New Normal

FDA Wards of Security Flaw in **Infusion Pump**

Major Retailer Hacked

Retailer Spends $100M in Light of Attacks

14 million vehicles recalled after hack

70M Customers Effected in Data Breach

40M Credit Cards Stolen

CIO and CEO Resign in Data Breach Failure
Cisco's Threat-Centric Security Model

Covers the Entire Attack Continuum

**BEFORE**
- Discover
- Enforce
- Harden

**DURING**
- Detect
- Block
- Defend

**AFTER**
- Scope
- Contain
- Remediate

Security Services

- Firewall
- Application Control
- Secure Access + Identity Services
- VPN
- Policy Management

- NGIPS
- DDoS
- Web Security
- Email Security

- Advanced Malware Protection
- Malware Sandboxing
- Network Behavior Analysis
Massive Innovation and Investment over Last 15 months

- AMP Everywhere
- Cisco ASA with FirePOWER Services
- Network as a Sensor and Enforcer
- New Platforms (ASA 5506, 5508, 5516, 5506-H, & FirePOWER 9300)

- Elastica, RadWARE, and ZIX partnerships
- FirePOWER Services on ISR
- ThreatGRID appliance
- Neohapsis and Portcullis Acquisitions
- Advanced Threat Analytics

- ACI Integration with ASA and FirePOWER
- OpenDNS and Lancope Acquisition
- Hosted Identity Services
- AMP in AnyConnect

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Why Global Service Providers Choose Cisco

“Our approach to how we counter threats in terms of our architecture has pointed us toward consolidation of our infrastructure. That’s where we have a very vibrant partnership with Cisco.”

“Cisco has made some really smart acquisitions of Sourcefire, Threat Grid, Cognitive, and of the new FirePOWER NGIPS product now provide a differentiated capability in the marketplace.”

“The opportunity in front of us is to build rapidly and advance rapidly on our ability to deliver protection to our customers in a way which working with other partners we can’t do.”
Best of Breed Portfolio
Architectural Approach

The Cisco Advantage
Integrated Threat Defense
Dynamic Threat Landscape – Customers Biggest Security Challenges

A community that hides in plain sight avoids detection and attacks swiftly

- 60% of data is stolen in HOURS
- 85% of point-of-sale intrusions aren’t discovered for WEEKS
- 54% of breaches remain undiscovered for MONTHS
- 51% increase of companies reporting a $10M loss or more in the last YEAR
- 100% of companies connect to domains that host malicious files or services last YEAR

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Threat-Centric Architectural Approach

A Continuously Evolving Threat Landscape…

…Requires an Integrated Threat Defense Architecture

- Faster Time to Detection, Faster Time to Contain
Speed Matters – Time to Detect

Industry: 200 DAYS

VS

Cisco: 46 HOURS

Cisco Minimizes The Time to Detect Breaches
Beyond the Event Horizon

Point-in-time Detection

Antivirus
Sandboxing

Initial Disposition = Clean

Analysis Stops

Retrospective Detection, Analysis Continues

Continuous

Initial Disposition = Clean

Addresses limitations of point-in-time detection

Actual Disposition = Bad = Blocked

Blind to scope of compromise

Turns back time

Visibility and Control are Key

Sleep Techniques
Unknown Protocols
Encryption
Polymorphism

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Advanced Malware Protection Everywhere

- Coming Q1CY16
  - Meraki MX
- Dedicated FirePOWER Appliance
- Web & Email Security Appliances
- FirePOWER Services on ISR
- FirePOWER Services on ASA

Best-in-Class Detection

Leader in Security Effectiveness

Broadoest Deployment Options

- Mac OS X
- PC
- AnyConnect
- Mobile
- Virtual
- Cloud Based Web Security & Hosted Email
- Private Cloud
Threat Centric NGFW

- We Block More
  - We block 99.2% of exploits per NSS NGFW test
  - Shrink Detection from 200 Days to 46 Hours

- We Prioritize Better
  - Enables quick focus on the alerts that matter
  - Endpoint plus Network correlation

- We Integrate Better
  - Clustering & HA models
  - SDN Fabric integration
  - ISE Integration for Policy

Open Platform – APIs, Open Source, 3<sup>rd</sup> Parties
Bringing the Market with us…
CSTA (Cisco Security Technology Alliance) Ecosystem Partners
Cisco’s Integrated Threat Defense Architecture

- **ANALYTICS LAYER**
  - Global & Local Threat Intelligence (Talos)
  - Raw Data (Cisco + 3rd Party)
  - Threat Research
  - Analytics Engines

- **SERVICES LAYER**
  - Integrated Management

- **ENFORCEMENT LAYER**
  - Security Services Layer
  - Network Platforms
  - Cloud Platform
  - Endpoint Platform

- **Integration Points**
  - Policy Automation and Controller Integration

- **Behavioral Threat Analytics**
- Network Behavioral Analytics
- Network Enforcement & Malware Detection
- Malware Sandboxing (Adv. Threat Protect.)
- 24x7 Visibility & Enforcement.
- Global Intelligence and Research.
Why OpenDNS?
OpenDNS Sees the Entire Internet
DNS is the fastest way to establish Security Everywhere
DNS is *Used by Every Device* on Your Network
OpenDNS
PRODUCTS & TECHNOLOGIES

UMBRELLA
Enforcement
Network security service protects any device, anywhere

INVESTIGATE
Intelligence
Discover and predict attacks before they happen

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
OpenDNS Adds to Cisco’s Security Portfolio

Attack Continuum

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

OpenDNS Umbrella

OpenDNS Investigate
Stay ahead of future attacks by blocking malicious domains, IPs, and ASNs

OpenDNS Investigate
Block callbacks on any port, protocol, or app at the DNS & IP layers

OpenDNS Investigate
Query live threat intelligence of all the domains & IPs on the internet.

© 2014. Cisco and/or its affiliates. All rights reserved. Cisco Confidential
OpenDNS Delivers Worldwide Coverage in Minutes

208.67.222.222
208.67.220.220
OpenDNS & IoT (Device / Entity) Protection

- No endpoint client / All IoT can use DNS.
- Seamless, secure, global visibility for millions of IoT devices.
- Powerful, light approach to global IoT threat enforcement.
Integration of Threat Grid and Umbrella

- **Customer & Partner Community**
- **Threat Detection & Intelligence**
  - AMP Threat Grid - Cloud
- **Umbrella Enforcement & Visibility**
  - Automatically Pulls newly discovered malicious domains in minutes
  - Logs or Blocks all Internet activity destined to these domains
Cisco Announces Agreement to Acquire Lancope
# About Lancope

<table>
<thead>
<tr>
<th><strong>Web Site</strong></th>
<th><a href="https://www.lancope.com">https://www.lancope.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>History</strong></td>
<td>Founded 2000</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>Privately held</td>
</tr>
</tbody>
</table>
| **Key Talent and Location** | - Mike Potts, CEO  
- Tim Keanini, CTO  
- David Cocchiara, COO/CFO  
- David Scruggs, VP Sales  
  Headquartered in Alpharetta, GA. |
| **No. of Employees** | ~300 employees |
| **Customers** | Blue Chip customer base, including financial services, healthcare, retail, technology, manufacturing, education, service providers, and other enterprises |
Lancope Adds to Cisco’s Security Portfolio

Attack Continuum

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Lancope
Discover and monitor traffic baseline for the network
Leverage awareness to apply more granular controls

Lancope
Detect Breaches and Insider Threat Faster
Accelerate the analyzing and understanding of incidents
Lancope StealthWatch System


**Monitor**
- Understand your network and data center normal
- Gain real-time situational awareness of all traffic
- Network segmentation and policy instrumentation

**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
Roadmap Highlights
Security Road Map Quick Highlights

Q3/Q4 CY15
- Unified Image and Offbox Mgmt
- NG DC Platform: 3RU – FP9300
- Network as a Enforcer Work Center in ISE

Q1 CY16
- Next Gen Onbox Manager
- 1RU High Perf Model
- AMP ThreatGRID appliance Integration across Portfolio

Q2 CY16
- Next Gen 1RU for Midrange
- Multiple Integrated Threat Defense Capabilities
- AMP Private Cloud Integrations across Portfolio
- Offnet coverage for Network as a Sensor via AnyConnect
- ACS Capabilities (TACACS+ Lite)
Cisco Security Portfolio

Integrated Threat Defense Architecture

Open | Pervasive | Integrated | Continuous
Thank You