Service Provider Webinar Series
Security Session

Paolo Poggi, Consulting Systems Engineer Security
The Agenda

Cisco Security Story

Security Solutions That Every SP Customer Wants and Needs

Next Steps
Cisco Security Story
Cisco is Investing in Security Growth

- PIX Firewall which was foundation of current ASA-X
- Top Leader of contents security
- Snort®, ClamAV®, Open source projects Founder VRT World-class research Top Leader of IPS
- Top Leaders of security advisory services Provides risk management and compliance to Fortune 500 customers
- Leading Dynamic Malware Analysis (Sandbox) Currently Integrated to AMP
- Cloud-native ML techniques for device modeling identifies insider and external threats faster and more accurately.
- Cloud based DNS security service
- Cloud Managed Secure Converged Infrastructure for Cloud Connector Apps.
- Cloud-based DNS security service
- Leading Cloud security platform that provides visibility and control for SaaS, IaaS and PaaS
- Leading security analytics platform to defend against advanced cyber threats
- Zero-trust security Platform
Cisco Security Commitment (among +2,500 vendors)
Cisco Security Commitment (among +2,500 vendors)
SECURITY EVERYWHERE

Attack Continuum

Before       During       After

Endpoint    Branch    Edge    Campus    Data Center    Cloud    Mobile IoT

Security Services
### Cisco Security Solutions: Simple / Automated / Open

**Before DURING AFTER**

#### Local Visibility Sharing / Management / Orchestration

*Cisco pxGRID API, REST API*

- **Detect & Control**
  - NGFW / NGIPS / APT - Cisco Firepower with Anti Malware (AMP)
  - Web / Email - Cisco Content Security
  - Analytics, UEBA - Cisco Stealthwatch, CTA, Tetration
  - CASB - Cisco Cloudlock
  - NAC/Security Policy - Cisco ISE
  - RA VPN - Cisco AnyConnect
  - The Network and Cloud - Cisco Switches, Wireless, Routers, Meraki, OpenDNS Umbrella

- **Identify & Block**
  - Analysis & Remediation

- **Analysis & Remediation**

**Mgmt API**

**Threat Intel API**

### Global Visibility & Threats Intelligence

*Cisco TALOS*
Why Security Architecture? SP Security Challenges

- Complexity, Fragmentation
- Attack surface too broad
- Lack of Security Orchestration
- Threats sophistication
- Lack of threats visibility
Why Security Architecture? SP Security Challenges

- Complexity, Fragmentation
- Attack surface too broad
- Lack of Security Orchestration
- Threats sophistication
- Lack of threats visibility

~50 Security Vendors at different endpoints: Silos aren’t simplifying protection
The Security Product Efficacy

The security product **efficacy**

= 

The quality of vendor’s Threat Intelligence
Superior Threat Intelligence

Continually updates Cisco NGFW, informed by our full security architecture

Visibility  Radware DDoS  URL  Network analysis  Email  Threats  Identity and NAC  DNS  Firewall

20 billion
Threats blocked daily

1.5 million
Daily malware samples

600 billion
Daily email messages

16 billion
Daily web requests

24 • 7 • 365 operations

300+
Full time threat intel researchers

Millions
Of telemetry agents

4
Global data centers

Over 100
Threat intelligence partners
Security Solutions That Every SP Customer Wants and Needs
1) Next Generation Firewalls
Harden and secure networks against advanced threats

NGFW for:
- Campus
- Internet Edge,
- Cloud DC edge
- Local DC edge
- Core Network/EPC
- Acceptable use
- ACI integration
- Remote access
- Rapid Threat Containment

Traditional Firewall
- Advanced Clustering
- Policy Control
- NAT and ACLs

Next Gen Firewall (NGFW)
- Context Awareness
- SSL Decryption
- File Type Blocking

with Intrusion Prevention (IPS)
- Threat Discovery and App Control
- Threat Analysis
- Threat Management

© 2018 Cisco and/or its affiliates. All rights reserved.
The Network platform uses indications of compromise (IoC), file analysis and in this example file trajectory to show you exactly how malicious files have moved across the environment.
Security Platforms for Service Providers

Cisco Firepower is a threat-centric security solution that offers tight integration, end-to-end automation, and enhanced agility on the same platform architecture.

- **ASA/FTD**
  - Firepower 9300 Series
  - Firepower 4100 Series
  - Firepower 2100 Series

- **ASAv / FTDv**
  - Virtual Appliances

© 2018 Cisco and/or its affiliates. All rights reserved.
Cisco Firepower 2100 Appliances FTD


Addressing 1GE-10GE connectivity
Cisco Firepower 4100 Appliances FTD


Addressing 1GE-10GE-40GE connectivity

Firepower 4110
12 Gbps AVC
10 Gbps AVC+IPS

Firepower 4120
20 Gbps AVC
15 Gbps AVC+IPS

Firepower 4140
25 Gbps AVC
20 Gbps AVC+IPS

Firepower 4150
30 Gbps AVC
24 Gbps AVC+IPS
Cisco Firepower 9300 Appliances FTD


Addressing 1GE-10GE-40GE-100GE connectivity
Cisco ASA and Firepower Threat Defense Virtual

vmware
ESXi

amazon
web services

KVM

Azure
Positioning the Firepower NGFW

Refresh with Firepower 2100

If you have
ASA 5525-X/ ASA 5545-X/
ASA 5555-X

Firepower 2100 series

Refresh it with
Firepower 2110/2120
Firepower 2130/2140

2100 Series available with either
ASA OR Firepower Threat Defense (FTD) software.

Evolve to the Firepower 4100

If you have
ASA 5585-X

Firepower 4100 Series

Refresh it with
Firepower 4110/4120
Firepower 4140/4150
Firepower 9300

4100 Series available with either
ASA OR Firepower Threat Defense (FTD) software.
Management Overview

- Chassis management is independent from applications
  1. On-box chassis manager UI, CLI, and REST API
  2. SNMP and syslog support for chassis level counters/events on Supervisor (FP4100 and FP9300)

- Applications are managed through their respective interfaces
  1. CLI, REST API, ASDM, and off-box Cisco Security Manager for ASA
  2. Off-box Firepower Management Center (FMC) for FTD
2) (Radware) DDoS
Radware Virtual DefensePro (vDP)

- Provides protection against Application layer attacks and State-table exhaustion attacks – Low/Slow DDoS
- Primarily deployed to protect the firewall itself and the application servers behind it
- For volumetric attacks vDP can transfer the attack traffic signature to the Cloud along with the clean traffic profile for near instant mitigation.

Available Services
- Network
  - Behavioral DoS
  - Real Time Signature
  - Network Challenge Response
  - Behavioral Anti-Scan
- Server
  - Behavioral DNS Protection
  - DNS Challenge Response
  - SSL Session and Network Protection
  - Advanced Fingerprinting
- Application
  - Behavioral HTTP Flood Protection
  - HTTP Polymorphic Challenge Response
  - Encrypted Challenge Response

www.radware.com/partners/technologypartners/cisco-firepower-ngfw
Cisco Firepower with Radware

- Integrated Radware Virtual DefensePro (vDP) in-line DDoS mitigates attacks
- Available on Cisco Firepower 4100 Series & Firepower 9300 platforms running ASA or FTD
- Lower latency than a stand-alone DDoS solution
- Consolidation with simplified support and procurement
Cisco Radware Portfolio

As-A Solution (HW/SW)  
Managed Service

ADC/SSL

WAF

DDoS

Single Pane of Glass Management

Service-Level Visibility

Automation & Orchestration

© 2018 Cisco and/or its affiliates. All rights reserved.
Why You Should Care

- DDoS still a massive issue for every places on the Internet
- Slow and Low protection, not just about volumetric attacks
- Every SP deals with DDoS, whether they know it or not
- IoT attacks on the rise
- Customers need protection, and this protection leads to other security and network sales
3) Software and Cloud Solutions: AnyConnect, AMP, Umbrella, ISE, Cloudlock
Cisco AnyConnect® – Way more than VPN

AnyConnect® features

Basic VPN  Advanced VPN  Endpoint Compliance  Enterprise Access  Threat Protection  Network Visibility  Roaming Protection

Cisco AnyConnect

Integration with other Cisco solutions


© 2018 Cisco and/or its affiliates. All rights reserved.
AMP Cisco Security Ecosystem
Powered by Talos Cisco's industry-leading threat intelligence group

AMP for Email
O365 Integration

AMP for Content
CTA Integration

AMP for Networks

AMP for Endpoints
AMP Visibility
CTA Integration
New

AMP for Umbrella
DNS Protection

AMP Threat Grid
Unified Malware Analysis and Threat Intelligence

See once, block everywhere
Track active processes and see history (incident response)
Cisco Umbrella – Security Made Easy

Benefits
- Block malware before it hits the enterprise
- Contains malware if already inside
- Internet access is faster
- Provision globally in minutes
Cisco Identity Services Engine (ISE)

A centralized security solution that automates context-aware access to network resources and shares contextual data.

- Identity Profiling
  - Who
  - What
  - When
  - Where
  - How
  - Applications
  - Hardware
  - Context

- Access Policy
  - Traditional
  - Cisco TrustSec®

- Network Resources
  - Guest Access
  - Enterprise Mobility (BYOD)
  - Secure Access
  - Device Administration

- See who and what is on your network
- Share information to bolster security
- Provide software-defined segmentation
- Rapidly respond and contain threats

ISE pxGrid Controller
CASB – API Access (OAuth)
4) Stealthwatch and Stealthwatch Cloud
Effective security is dependent on the ability to see everything in your network

- KNOW every host
- SEE every conversation
- Understand what is NORMAL
- Be alerted to CHANGE
- Respond to THREATS quickly

SW Use Cases: https://community.cisco.com/t5/security-documents/stealthwatch-use-cases/ta-p/3611837
5) Incident Response
Cisco Incident Response (IR) Services

Needed when Security Breach occurs with your customer!

- **Incident Response Retainers**
  - I want to know I have a team standing by

- **Emergency Incident Response**
  - In need help now

- **Proactive Threat Hunting**
  - I need to know what is in my network

- **IR Tabletop Exercises**
  - I need a plan for when a data breach occurs

- **IR Readiness Assessments**
  - I need to know if I can respond appropriately

Included in the Cisco IR

Next Steps
## Free Trials and Assessments

[Click here for more...](#)

### Search all offers and trials

<table>
<thead>
<tr>
<th>Offer</th>
<th>Description</th>
<th>Technology</th>
<th>Type of offer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Umbrella</td>
<td>Your first line of defense at half the cost</td>
<td>Cisco DNA Security</td>
<td>Promotional Offer</td>
</tr>
<tr>
<td>Stealthwatch Assessment</td>
<td>Stealthwatch free 2-week visibility assessment.</td>
<td>Cisco DNA Security</td>
<td>Assessment</td>
</tr>
<tr>
<td>Identity Services Engine</td>
<td>ISE 2.0 Trial Offer. Demo of ISE capabilities + Business case walkthrough.</td>
<td>Cisco DNA Security</td>
<td>Free Trial</td>
</tr>
<tr>
<td>Next Gen Firewall Free Evaluation &amp; Scan</td>
<td>Free 2-week trial (US only).</td>
<td>Cisco DNA Security</td>
<td>Free Trial</td>
</tr>
<tr>
<td>Cisco Umbrella</td>
<td>14 Day Free Trial of Cisco Umbrella.</td>
<td>Cisco DNA Security</td>
<td>Free Trial</td>
</tr>
</tbody>
</table>

Follow us [Social Media Icons]
Hands on Lab with Cisco dCloud

dCloud hands on lab & demo (Stealthwatch, Umbrella, AMP, ISE, Firepower) - https://dcloud.cisco.com
(Register, enter your login, search “Stealthwatch”, “Tetration Analytics” and select the demo / lab you would like to try on)
What if defenders could see the future? If they knew an attack was coming, they could stop it—or at least, mitigate its impact and ensure what they need to protect most is safe. The fact is, defenders can see what’s on the horizon. Many clues are out there—and obvious.

Download the Cisco 2018 Annual Cybersecurity Report:
http://www.cisco.com/go/acr2018
Lo stato della sicurezza informatica in Italia
200 aziende italiane hanno condiviso con i nostri esperti le sfide e le opportunità che affrontano ogni giorno. Ecco i risultati

Engage with your local Cisco team to discuss the SP business models available