GSP Webinar Series
Security Session

Gabriel Agatiello, CyberSecurity Specialist
gagatiel@cisco.com
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

1995

Top Leader of contents security

2007

Sprint®, ClamAV®, Open source projects Founder VRT World-class research Top Leader of IPS

2009

Snort®, Snort ClamAV®, ClamAV® Open source projects Founder VRT World-class research Top Leader of IPS

2013

Snort®, ClamAV®, Open source projects Founder VRT World-class research Top Leader of IPS

2014

Top Leaders of security advisory services Provides risk management and compliance to Fortune 500 customers

2015

Leading Dynamic Malware Analysis (Sandbox) Currently Integrated to AMP

2016

Cloud-based DNS security service

2017

Cloud Managed Secure Converged Infrastructure for Cloud Connector Apps.

2018

Cloud-native ML techniques for device modeling identifies insider and external threats faster and more accurately.

2019

Leading security analytics platform to defend against advanced cyber threats

2020

Leading Cloud security platform that provides visibility and control for SaaS, IaaS and PaaS

2021

Zero-trust security Platform
Cisco Security Commitment (among +2,500 vendors)
Cisco Security Commitment (among +2,500 vendors)
SECURITY EVERYWHERE

Attack Continuum

Before

Branch

Edge

Campus

Data Center

Cloud

Mobile IoT

After

Endpoint

Security Services

Cisco

© 2016 Cisco and/or its affiliates. All rights reserved.
Best of breed portfolio

- UTM
- Network Analytics
- Cloud Access
- Secure Internet Gateway
- Email Security

Key Features:
- Simple
- Open
- Automated
- Effective

Threat Intelligence

Best of breed portfolio

- UTM
- Network Analytics
- Cloud Access
- Secure Internet Gateway
- Email Security

Key Features:
- Simple
- Open
- Automated
- Effective
Superior Threat Intelligence

- 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

https://www.talosintelligence.com/
Why Security Architecture? SP Security Challenges

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

Multiple Management Paradigms
Multiple Identity Stores
Isolated Threat Intelligence
Inconsistent Enforcement

Home, On-the-go, Office / Factory
edge
Enterprise DC
Comm. / SMB / Branch
SP Core/ Edge
SP Cloud

SAAS
box
Salesforce
SP-1
SP-2
CSR
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

AMP
Admin
Firepower Management Center
Malware Protection Across Networks with AMP

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.

- **Firepower 9300 Series**: ASA/FTD
- **Firepower 4100 Series**: ASA/FTD
- **Firepower 2100 Series**: ASAv / FTDv
- **Virtual Appliances**
Cisco Firepower 2100 Appliances FTD

Addressing 1GE-10GE connectivity

Cisco Firepower 4100 Appliances FTD

Cisco Firepower 9300 Appliances FTD


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

**Refresh with Firepower 2100**
- If you have ASA 5525-X/ASA 5545-X/ASA 5555-X
  - Refresh it with Firepower 2110/2120, Firepower 2130/2140
- Firepower 2100 series available with either ASA or Firepower Threat Defense (FTD) software.

**Evolve to the Firepower 4100**
- If you have ASA 5585-X
  - 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
Why We Should Care:

• Refresh Opportunity
• Firepower Matters
• Many older solutions going EOS / EOL
• NGFW drives Enterprise Networking deals
2) Cisco+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

<table>
<thead>
<tr>
<th>Network</th>
<th>Server</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavioral DoS</td>
<td>Behavioral DNS Protection</td>
<td>Behavioral HTTP Flood Protection</td>
</tr>
<tr>
<td>Real Time Signature</td>
<td>DNS Challenge Response</td>
<td>HTTP Polymorphic Challenge Response</td>
</tr>
<tr>
<td>Network Challenge Response</td>
<td>SSL Session and Network Protection</td>
<td></td>
</tr>
<tr>
<td>Behavioral Anti-Scan</td>
<td>Advanced Fingerprinting</td>
<td>Encrypted Challenge Response</td>
</tr>
</tbody>
</table>

[www.radware.com/partners/technologypartners/cisco-firepower-ngfw](http://www.radware.com/partners/technologypartners/cisco-firepower-ngfw)
Cisco Firepower Threat Defense
Prevent network and application downtime

Cloud scrubber

Flood traffic
- SYN flood attacks
- DDoS attacks
- Nonstandard packet attacks

Legitimate traffic

Network and applications

Maintain up to 42 Gbps
total mitigation capacity
Handle 627,000
customes per second
Block 5,400,000 packets
of flood traffic per second

Stop attacks within seconds of detection
Block or allow traffic automatically

* Radware DDoS supported in 4100 & 9300 families
Cisco Radware Portfolio

ADC/SSL

WAF

DDoS

Single Pane of Glass Management

Service-Level Visibility

Automation & Orchestration
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

**Basic VPN**

**Advanced VPN**

**Endpoint Compliance**

**Enterprise Access**

**Threat Protection**

**Network Visibility**

**Roaming Protection**

**AnyConnect® features**

**Cisco AnyConnect**

Integration with other Cisco solutions

- ISR
- ASR / CSR
- Adaptive Security Appliance (ASA)
- Identity Services Engine (ISE)
- Security Services (WSA)
- Switches and Wireless Controllers
- Advanced Malware Protection
- Netflow Collectors
- Umbrella Services
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

AMP
See once, block everywhere

© 2018 Cisco and/or its affiliates. All rights reserved. 31
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

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

<table>
<thead>
<tr>
<th>Secure Access</th>
<th>Traditional</th>
<th>Cisco TrustSec®</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Mobility (BYOD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Administration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Network Resources

- Share information to bolster security
- Rapidly respond and contain threats

© 2018 Cisco and/or its affiliates. All rights reserved.
# What can ISE deliver?

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asset Visibility</strong></td>
<td>Cisco ISE can reach deep into the network to deliver superior visibility into who and what is accessing resources.</td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td>Consistent access control across wired, wireless and VPN Networks. 802.1X, MAC, Web Authentication and Easy connect for admission control.</td>
</tr>
<tr>
<td><strong>Guest Access</strong></td>
<td>Fully customizable branded mobile and desktop guest portals, with dynamic visual workflows to easily manage guest user experience.</td>
</tr>
<tr>
<td><strong>BYOD Access</strong></td>
<td>Simplified BYOD management with built-in CA and 3rd party MDM integration for onboarding and self-service of personal mobile devices</td>
</tr>
<tr>
<td><strong>Segmentation</strong></td>
<td>Topology independent Software-defined segmentation policy to contain network threats.</td>
</tr>
<tr>
<td><strong>Context Exchange</strong></td>
<td>Context sharing with partner eco-system to improve their overall efficacy and accelerate time to containment of network threats.</td>
</tr>
<tr>
<td><strong>Threat Control</strong></td>
<td>Protection against threats across the attack continuum, before, during and after an attack. Reduce time-to-detection from days to hours.</td>
</tr>
<tr>
<td><strong>Device Admin</strong></td>
<td>Cisco ISE supports device administration using the TACACS+ security protocol to control and audit the configuration of network devices</td>
</tr>
</tbody>
</table>

© 2018 Cisco and/or its affiliates. All rights reserved.
CASB – API Access (OAuth)

- Managed Users
- Managed Devices
- Managed Network
- UnManaged Users
- UnManaged Devices
- UnManaged Network

Cisco NGFW / Umbrella

PUBLIC API ACCESS

ADMIN OAUTH ACCESS

Authorized

Cisco Cloudlock
Why We Should Care

• Starts XaaS, Endpoint, Day 0, other conversations
• Relatively high impact, low cost
• Software drives hardware
4) Stealthwatch and Stealthwatch Cloud
Secure digital businesses demand increased visibility

- Know every host
- Record 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
Security Analytics with Stealthwatch

**Data collection**
Rich telemetry from the existing network infrastructure

**Global threat intelligence**
(powered by Talos)
Intelligence of global threat campaigns mapped to local alarms for faster mitigation

**Multilayered machine learning**
Combination of supervised and unsupervised techniques to convict advanced threats with high fidelity

**Behavioral modeling**
Behavioral analysis of every activity within the network to pinpoint anomalies

**Encrypted Traffic Analytics**
Malware detection without any decryption using enhanced telemetry from the new Cisco devices
Why We Should Care

- SOVA
- Visibility
- Account stickiness
- Control over the network and the cloud
- Can be used to position many Cisco Security Solutions – not just Stealthwatch
5) Incident Response
Cisco Incident Response (IR) Services

Needed when Security Breach occurs with your customer!

<table>
<thead>
<tr>
<th>Incident Response Retainers</th>
<th>Emergency Incident Response</th>
<th>Proactive Threat Hunting</th>
<th>IR Tabletop Exercises</th>
<th>IR Readiness Assessments</th>
</tr>
</thead>
<tbody>
<tr>
<td>I want to know I have a team standing by</td>
<td>In need help now</td>
<td>I need to know what is in my network</td>
<td>I need a plan for when a data breach occurs</td>
<td>I need to know if I can respond appropriately</td>
</tr>
</tbody>
</table>

Included in the Cisco IR

Next Steps
Cisco Security Assessment Menu
Free Security Offers in 2018

No matter where you are on your security journey, there’s a solution for you.

The best part is trying it for free and learning as you go.

Contact your Cisco Security Account Team to enable these free assessments.

# Free Trials and Assessments

## 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>enter search term</td>
<td>enter search term</td>
<td>Cisco DNA Security</td>
<td>View All</td>
</tr>
<tr>
<td>Cisco Umbrella</td>
<td>Your first line of defense at half the cost</td>
<td></td>
<td></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

---

FOLLOW US  
Twitter   
Facebook  
Instagram  
LinkedIn   
YouTube   

Newsroom  
Events  
Blogs  
Community  

© 2018 Cisco and/or its affiliates. All rights reserved. 46
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”, etc… 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.

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