The Security Session
The Agenda

Cisco Security Story

The 5 Security Solutions That Every SP Customer Wants and Needs

Next Steps
The Cisco Security Story
Cisco is Investing in Security Growth

- PIX Firewall which was foundation of current ASA
- 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
- Cloud based DNS security service
- Cloud based network forensics and visibility
- Top Leader of Cloud-based Web Security
- Leading Dynamic Malware Analysis (Sandbox)
- Currently Integrated to AMP
- Leading security analytics platform to defend against advanced cyber threats
- Leading Cloud security platform that provides visibility and control for SaaS, IaaS and PaaS
SECURITY EVERYWHERE

Attack Continuum

Before

During

After

Endpoint
Branch
Edge
Campus
Data Center
Cloud
Operational Technology

Services
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**

- **250+**
  Full time threat intel researchers
- **Millions**
  Of telemetry agents
- **4**
  Global data centers
- **Over 100**
  Threat intelligence partners

© 2017 Cisco and/or its affiliates. All rights reserved.
Best of breed portfolio

Network Analytics

UTM

Cloud Access

Secure Internet Gateway

Email Security

Advanced Malware

NGFW/NGIPS

Network Access

Web

© 2017 Cisco and/or its affiliates. All rights reserved.
The 5 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
- 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
- Threat Discovery and App Control
- Threat Analysis
- Threat Management

with Intrusion Prevention (IPS)

AMP

Admin

Firepower Management Center

© 2018 Cisco and/or its affiliates. All rights reserved.
Protection Across Networks

The Network platform uses indications of compromise, file analysis, and in this example file trajectory to show you exactly how malicious files have moved across the environment.
Cisco Next-Gen Firewall: Hardware/Software Options

**Performance and Scalability**

**SMB & Distributed Enterprise**
- ASA 5506H-X
- ASA 5506W-X
- ASA 5506-X
- ASA 5508-X

**Mid-Range**
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X

**Data Center, High Performance Computing, Service Provider**
- Firepower 9300:
  - SM24
  - SM36
  - SM44
- Firepower 4100:
  - 4110
  - 4120
  - 4140
  - 4150
- Firepower 2100:
  - 2110
  - 2120
  - 2130
  - 2140
- ASAv (VMware, KVM, AWS, Azure, Hyper-V)
- FTDv (VMware, KVM, AWS, Azure)
- IPS/IDSv (VMware, ISR)
- Radware

**ASA 5585-X EoS – Promo FP2100/4100 Series with ASA/FTD**
Choose the Firepower NGFW that’s right?

**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

4100 Series available with either ASA OR Firepower Threat Defense (FTD) software.
Why We Should Care:

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

<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>
Cisco Firepower with Radware

- Integrated Radware Virtual DefensePro (vDP) in-line DDoS mitigates attacks
- Available on Cisco Firepower 4100 Series & Firepower 9300 platforms
- Lower latency than a stand-alone DDoS solution
- Consolidation with simplified support and procurement
Why We Should Care

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

AnyConnect® features

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 Umbrella
DNS Protection

AMP for Endpoints
AMP Visibility
CTA Integration

New

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
  - 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
CASB – API Access (OAuth)
Why We Should Care

- Starts XaaS, Endpoint, Day 0, other conversations
- Relatively high impact, low cost
- Software drives hardware
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
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!

- **Incident Response Retainers**
  - I want to know I have a team standing by
  - Typical Industry IR Retainers
  - Included in the Cisco IR Retainers

- **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

Retainer
CON-AS-SECADV
Next Steps
Cisco Security Assessment Menu
Free Security Offers in 2019

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.
Advanced Malware Protection (AMP) for Endpoints
Do you have visibility into the files and processes running on your endpoints? If a malicious file is downloaded and executed, are you able to track its history and actions? Take the next step past traditional antivirus with next-generation endpoint security.

Stealthwatch – Security Visibility Assessment
Is your network compromised today? How do you know? Take a two-week Security Visibility Assessment to identify risky network behavior such as traffic to high-risk countries, remote access breaches, and telnet usage.

Email Security with AMP
Scanning your email with Cisco Email Security? Have you had a policy review lately? We can assist you with a health check and trial run of AMP to help protect today’s #1 threat vector, email.
Next Generation Firewall (NGFW) - Threat Scan
Need to upgrade your firewall or help your customer see the benefits of our security architecture? Start with a free threat scan hosted by our security preferred partners. Sign up for a NGFW trial.

Stealthwatch Cloud - Free Trial
Easily identify threats in your public cloud infrastructure and private network – from a single screen. Stealthwatch Cloud provides visibility and threat detection in Amazon Web Services, Google Cloud Platform and Microsoft Azure.

Cloudlock - Security Assessment
Can your on-premises security protect cloud apps? Cisco Cloudlock quickly and easily helps protect your users, data and apps in the cloud against compromised accounts, data breaches and malware.

Umbrella - Free Trial
Do you want to reduce malware and make limited staff more efficient? Cisco Umbrella deploys in less than 30 minutes to help you identify and investigate threats faster, and protect users from threats on the internet, everywhere they go.
Engage with your local Cisco team to discuss the SP business models available
Extra
What is the Security Online Visibility Assessment (SOVA)?

The Security Online Visibility Assessment (SOVA) enables Customers to quickly and easily gain insight into networks, including areas of security risk.

SOVA uncovers the below *Indicators of Compromise* for customers:

- **Internal Monitored Network**: Key information about the internal network that can help scope for deployments.
  - AMP, ISE & STEALTHWATCH

- **Encrypted Traffic**: Threats often are ‘hidden’ inside Encrypted Traffic. When combined with ETA on the Catalyst 9K, anomalous behavior is uncovered.
  - AMP, ISE & STEALTHWATCH

- **SMB Risk**: Hosts with many SMB sessions with hosts outside the network, which is consistent with an infection.
  - AMP

- **DNS Risk**: Unauthorized DNS servers in use & hosts at risk of exposure, DNS malware, or data loss.
  - UMBRELLA

- **Remote Access Breach**: Hosts who may be the victim of a remote access breach & assesses the total inbound & outbound remote access traffic.
  - NGFW

- **Unclassified Servers**: Unknown servers could represent a security risk as they may not have the appropriate security policies applied to them.
  - ISE & STEALTHWATCH

- **Telnet Risk**: Discovers hosts using Telnet & assesses the total amount of Telnet traffic, broken down by inbound, outbound, & internal host-to-host.
  - STEALTHWATCH

- **Traffic to High Risk Countries**: Hosts communicating with outside hosts located in countries the customer has deemed high risk.
  - STEALTHWATCH

**INSIGHTFUL and ACTIONABLE**