Cisco Firepower Next-Generation Firewall

Security from the network out

Nicolas Dard
Product Management
March 2019
Today’s Presenters

John Malzahn
Senior Manager,
Service Provider
Solutions Marketing
Cisco Systems

Nicolas Dard
Senior Product
Manager, Cyber
Security
Cisco Systems
New perimeter

Old perimeter
Traditional Network: Endpoints, On-site Users, Servers, Apps

- Remote employees
- Cloud applications
- Mobile devices
- Hybrid cloud
- Personal devices
- Vendors and contractors
Network security: Our goal

World class **security** controls

In **every** place you need them

With **unified** policy and threat visibility
Consistent, world class security controls

Gartner named Cisco a Leader in the 2018 Intrusion Detection and Prevention Systems Magic Quadrant – and every year since 2014

Snort IPS

AMP malware detection and response

You see once, block everywhere
We analyze massive amounts of data – 19.7 billion threats blocked daily

Our real-time datasets are diverse, global, and live

600 Billion Email samples

16 Billion Web requests

3.4 Billion AMP queries

170 Billion Internet requests

80 Million Daily active users

12,000 Enterprise customers

160 Countries worldwide
50 international sites protected by a competitor’s firewalls
2 U.S. sites with a Cisco NGFW placed behind the competitor’s firewall
50 international sites down for two weeks
2 U.S. sites fully operational

NOTPETYA
Security controls...In every place you need them
## Unmatched breadth of portfolio

### Security that works together

<table>
<thead>
<tr>
<th>Network</th>
<th>User/Endpoint</th>
<th>Cloud</th>
<th>Customer SOC</th>
<th>Cisco Threat Intel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software-Defined NAC (IDENTITY SERVICES ENGINE)</td>
<td>Auth/SSO (DUO MFA) BYOD (DUO ACCESS) SDP (DUO BEYOND)</td>
<td>SIG/SWG (UMBRELLA) CASB (CLOUDLOCK) Workload Protection (TETRATION)</td>
<td>Incident Response (THREAT RESPONSE)</td>
<td>Internet Investigations (UMBRELLA INVESTIGATE)</td>
</tr>
<tr>
<td>NGFW (FIREPOWER) UTM (MERAKI MX) Web Security</td>
<td>EPP/EDR (AMP FOR ENDPOINTS) Email Security</td>
<td>Security Analytics (STEALTHWATCH)</td>
<td>File Investigations (THREAT GRID)</td>
<td>Talos</td>
</tr>
<tr>
<td>Security Analytics (STEALTHWATCH) NGIPS (FIREPOWER)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Secure Access

### Threat Defense

---

INSEC-2003
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public
Modern Security Architecture

- **Open APIs · Developer Environment · Services**
- **Management · Response**
  - Deploy
  - Detect
  - Investigate
  - Remediate
  - Policy

- **Enforcement Everywhere**
  - Network
  - Endpoint
  - Cloud
  - Application

- **Comprehensive Threat Intelligence**
  - Known Threats
  - Unknown/Zero-day

- **Technology Partners and other 3rd party threat feeds**

- **Continuous Trust Verification**
  - Users, devices, applications, and more
Security controls...with easy operations, unified policy and unified visibility/incident response
New operational model built on APIs

Achieve operational efficiency

Integrate with customer ecosystem

FDM and CDO use the FTD APIs

Everyone can use the APIs for automation

FDM

FTD

CDO

Homegrown or 3rd party tools

Automation scripts

FMC

© 2018 Cisco and/or its affiliates. All rights reserved.
Firepower Device Manager - Improved User Experience for single device management

- Wizard based guided Workflows
- Optimized for Mid-Market
- Co-exists with Cloud Management
- Manages Firepower Threat Defense on low- & mid-range platforms
Cisco’s integrated security solutions

Single dashboard for security policy
Cisco Defense Orchestrator (CDO)

Single dashboard for threat response
(ALL Security)
Cisco Threat Response
Cisco Defense Orchestrator (CDO)
Common capabilities across the network control point

Links the network edge together

Common Policy (CDO)

Secure Internet Gateway (Umbrella)

Dedicated Appliance (ASA, Firepower)

Network Embedded (Meraki, ISR)

High quality detection and inspection in all areas

AMP/TG
Snort
SSL Decryption
Stealthwatch/CTA
TALOS

Common Elements
Introducing Cisco Threat Response
Unleashing the power of the Cisco Integrated Security Architecture

Key pillar of our integrated security architecture

• Automates integrations across Cisco security products
• Reduces the time and effort spent on key security operations functions:
  - Detection
  - Investigation
  - Remediation
• Included as part of Cisco Security product licenses
Cisco Threat Response in the real world
Join Cisco Security customers who are gaining value from it now

2500+ Organizations are using it today

“I like quickly being able to see infections on my network, and this presents them in a really nice fashion...”

“You cannot hit a target you cannot see. Cisco Threat Response really simplifies security analysis...”
Firepower Improvements
Cisco Firewall is a leader in the 2018 Gartner MQ
NGFW: More Competitive Than Ever

6.2.3 Solid Foundation
- Fundamentally stable product with Focus on Quality & Hardening
- Visibility into encrypted web traffic - 75% of all web
- New Migration Experience from ASA to NGFW

6.3 FTD Acceleration
- Unlock Enterprise and Public Sector deals with Multi-instance
- Operational efficiency enhancements
- Simple, modern on-box UI for Mid-Market
- Launch of cloud-based event visibility tool

6.4 Competitive Advantage
- Price / performance enhancements
- Cloud Managed Mid-market Firewall
- Enhanced visibility tool to include malware events

API-First Approach & Predictable Feature Delivery
6.3 Key Deliverables

- **Multi-instance**
- Air gap/ export
- APIs
- FDM HA
- FQE from device

**Enterprise**
- Multi-instance
- Software performance improvements
- API for management scale

**Public Sector**
- Multi-instance
- Air gap licensing support
- Export control support

**Service Provider**
- Multi-instance
- GTP protocol extensions
- APIs for FP2100 management

**Commercial**
- Dramatically expanded FDM capabilities with HA support
Work smarter with Cisco NGFW automation

**Policy**  
Automated policy application and enforcement frees up time so you can focus on high priority items

**IPS Tuning**  
Automatic IPS tuning blocks more threats and reduces the volume of alerts

**Prioritized Threats**  
Prioritized threat alerts show you where to focus on what matters most

**Integrated Tools**  
Cisco’s integrated security tools share and correlate data automatically to see and stop threats
ASA To FTD Migration – New Tool

**Independent from FMC**
- Takes away the pain of installing another FMC for migration
- Independent windows executable
- Independent releases with enhancements and bug fixes

**Rest API based**
- Supports migration of features supported in FMC Rest API
- Will support migration to FDM in the future
- Scalable

**Improved Workflow and reporting**
- Ability to edit the configuration being migrated
- Pre and post migration reports
- Live running logs, graceful error handling and resume from failure
- Object conflict detection and resolution
For more information

Visit:

www.cisco.com/go/spsecurity
www.cisco.com/go/ngfw

or contact your Cisco account representatives
Questions?