Digitization is disrupting the SP business

- The world has gone mobile
- Traffic growth, driven by video
- Rise of cloud computing
- Machine-to-Machine
- Changing Customer Expectations
- Ubiquitous Access to Apps & Services
- Exponential Growth in Data
  - More and more Data
  - More and more ways to access Data
  - More and more regulations on securing Data

Risks to Service Providers and Their Customers
All Data has Monetary Value

Global Cybercrime Market: $450B–$1T

- Social Security: $1
- Medical Record: >$50
- Credit Card Data: $0.25–$60
- Bank Account Info: >$1000 depending on account type and balance
- DDoS as a Service: ~$7/hour
- DDoS
- Mobile Malware: $150
- Spam: $50/500K emails
- Exploits: $100k–$300K
- Facebook Account: $1 for an account with 15 friends
- Malware Development: $2500 (commercial malware)
- Exploits

Welcome to the Hackers’ Economy

Source: CNBC
Money Motivates Attackers
Organizations Are Under Attack and Malware Is Getting in

- Cybercrime is lucrative, barrier to entry is low
- Hackers are smarter and have the resources to compromise your organization
- Malware is more sophisticated
- Organizations face tens of thousands of new malware samples per hour

95% of large companies targeted by malicious traffic
100% of organizations interacted with websites hosting malware

- Phishing, Low Sophistication
- Hacking Becomes an Industry
- Sophisticated Attacks, Complex Landscape

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Being Breached Costs Dollars and Reputation

- **Loss for every 1k data files breached**: $87k
- **Average lost business cost per attack**: $1.45M
- **Of security breaches compromise data in hours**: 60%
- **Of security breaches are not detected until months later**: 54%

Loss of customer trust
Shift to 5G Will Be Led by New Services

**Ultra Reliability** (Wherever + Whenever)
- Broadband access in dense areas
  - Pervasive Video
- Broadband access everywhere
  - Average 1 Gbps per device
- Higher user mobility
  - High Speed Train
- Massive Internet of Things
  - Sensor Networks

**Ultra Capacity and Coverage**
- Ultra High-Speed (up to 10 Gbps to cell site)
  - Extreme real-time communications
    - Tactile Internet
  - Lifeline communications
    - Natural Disaster
  - Ultra-reliable communications
    - E-Health Services
  - Broadcast-like services
    - Broadcast Services

**Ultra Low Latency** (1 ms End-to-End)
- Broadband access everywhere
  - Average 1 Gbps per device

**Massive Device Connectivity**
New Services Mean New Threats

Threat Surface

- 2G
- 3G
- LTE
- 5G
Cisco: Committed to Security

- 5K People Strong
- 250 Threat Researchers
- 100x Faster Finding Breaches
- 19.7B Threats Blocked Daily
- 99% Security Effectiveness
- #1 Cisco Priority
- Billions Invested
- Ongoing Innovation
- Integrated Best of breed portfolio
- 88% Fortune 100 use Cisco Security
Traditional Security Needs to Keep Pace
Security
Remember This?
Look Inside

Or Maybe Not
Traditional Security Needs to Keep Pace

Once inside, who is talking to who?
Traditional Security Needs to Keep Pace

Industry Average Time to Detect 100 Days
Example Threats inside the Perimeter

- Insider
- Internal DoS
- Interception and Exploitation
- Exfiltration
Security begins with visibility

Who is on the Network?

You can’t protect what you can’t see

And what are they up to?
Because when it happens.....

Incident reported

WHO did this?
HOW long?
WHAT was accessed?
WHEN did it happen?
WHEN will we know?

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Evolution of Firewalls

How to increase visibility at the Firewall?
Evolution of Security

Firewall

NGFW

Architecture including NGFW
Cisco Open Network Architecture for 5G, IoT, Beyond

Service Creation
OSS | BSS

Cloud-Based Services, Applications
Public | Private Cloud and/or On-Prem

Business | IoT | Video | Mobile | Collaboration

Network Abstraction
Orchestration | Automation

Streaming Telemetry

Infrastructure
Physical & Virtual
Security in the Open Network Architecture

- Security Analytics
  - Monitoring & Anomaly Detection
- Policy & Segmentation
  - What **should** happen on the network
- Visibility
  - What **is** happening on the network

**Enforcement**
- Cloud Based Services
- Network Abstraction
- Infrastructure

**Visibility**
Mobility Security Architecture - Visibility

- LAN / WAN Infra WiFi / BYOD
- Access & Aggregation
- Enterprise Network
- Call Centres Retail presence
- Internet Edge
- Partner Edge
- Datacentre
- Public Cloud
- Management Network
- MPC/EPC

- IN (IMS,SigTran)
- GSM
- 3G
- LTE

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Policy & Segmentation defines
Who is allowed to talk to Who?
What are they allowed to talk about?
How are they allowed to talk?
When are they allowed to talk?
Policy and Segmentation is not just between segments but also within segments.
Mobility Security Architecture – Policy & Segmentation

- Access & Aggregation
- LAN / WAN Infra
- WiFi / BYOD
- Enterprise Network
- Call Centres
- Retail presence
- Internet Edge
- Partner Edge
- IN (IMS, SigTran)
- Services
- GSM
- 3G
- LTE
- MPC/EPC
- Datacentre
- Public Cloud
- Management Network

What is happening on the network

What should happen on the network

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Security Architecture - Analytics

What is versus what should be

What is happening on the network

What should happen on the network

LAN / WAN Infra, WiFi / BYOD
Call Centres Retail presence
Internal / External Cloud
Peering
Datacentre
Management Network

BSS (Billing & Mediation)
OSS Systems,
Customer Portals
NfV & Orchestration

Gi LAN

Control Plane (Diameter)
User Plane (SCTP, GTP)

Gi
IMS, SigTran

Access & Aggregation

Interconnect

Security

Analytics

Enterprise Network

Cloud

OLO

LAN

ON/OFF

Ran

WiMax

Telecom

Internet Peering

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Security Architecture - Analytics

What is versus what should be plus what threats do we know and what is normal behavior.

What is happening on the network

What should happen on the network

- LAN / WAN Infra
- WiFi / BYOD
- Interconnect
- IN (IMS, SigTran)
- Control Plane (Diameter)
- User Plane (SCTP, GTP)
- MPC/EPC
- Management Network

Network

- Call Centres
- Retail presence
- Internet Peering
- Peering

Gi LAN

- Gi LAN

Datacentre

- Cloud
- Internal / External Cloud

- BSS (Billing & Mediation)
- OSS Systems
- Customer Portals
- NfV & Orchestration

Threat Intel

Access & Aggregation

- LAN / WAN Infra
- WiFi / BYOD

What is happening on the network

What should happen on the network
Security Architecture - Analytics

Analytics

What is versus what should be plus what threats do we know and what is normal behavior

Visibility

What is happening on the network

Policy

What should happen on the network

Threat Intel

LAN / WAN Infrastructure
WIFI / BYOD

Internet Peering

Gi LAN

Peering

Datacentre

Cloud

Management Network

Call Centres
Retail presence

BSS (Billing & Mediation)
OSS Systems,
Customer Portals
NfV & Orchestration

Gi / LO Interconnect

IN (IMS, SigTran)

Control Plane (Diameter)
User Plane (SCTP, GTP)

MPC/EPC

Management Network

What is happening on the network

What should happen on the network
Security Architecture

What is versus what should be plus what threats do we know and what is normal behavior

Visibility

What is happening on the network

Policy

What should happen on the network

Analytics

Service Change via Orchestration

Infrastructure Change via Orchestration

Enforcement Action to Mitigate Threat

Security Trigger

What should happen on the network

Service Change

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 30
Security in the Open Network Architecture

- Security Analytics
- Monitoring & Anomaly Detection
- Policy & Segmentation
- What **should** happen on the network
- Visibility
- What **is** happening on the network
- Cloud Based Services
- Security Driven Service Change
- Network Abstraction
- Security Auto-Remediation
- Infrastructure
Example

Enforcement

Firewall Rules

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Employee</td>
<td>Any</td>
</tr>
<tr>
<td>Any</td>
<td>Suspicious</td>
<td>Any</td>
</tr>
</tbody>
</table>

NGFW

Device is quarantined for remediation or mitigation – access is denied per security policy.

Datacenter Server

Based on the new policy, network enforcers automatically restrict access.

Device is compromised

Tries to breach datacenter

Visibility

User Activity and File Activity monitored, aggregated and analyzed.

Analytics

Analytics detect suspicious behavior and inform policy server.

Policy server changes policy for device

Policy

Rapid Threat Containment
Visibility

Which User Accessed a URL at any particular time?
Visibility

Cisco Stealthwatch

Correlates multiple data types and sources to provide traffic details, subscriber info and application context for every traffic flow passing through the network.
See Once, Enforce Everywhere
Protecting Network, Cloud, Device for 5G, IoT, Beyond

Security Gateway (SecGW) Solutions for Secure Mobile Backhaul

Centralized SecGW
- Firepower 9300
- Firepower 4100 Series
- ASA

Distributed SecGW
- ASR 900 Series
- ASA

Superior Performance and Scale
- High throughput IPsec VPN and Security Gateway processing

Exceptional Flexibility
- Right sized with pay-as-you-grow options; unique clustering technology on Firepower to optimize performance while reducing rack space, power and cooling costs

Future Proof
- Physical and virtual options to address architectural requirements

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Protecting Network, Cloud, Device for 5G, IoT, Beyond
Cisco Umbrella for New Revenue Opportunities

Cisco Umbrella for Service Providers

Learn
Intelligence to see attacks before they launch

See
Visibility to protect access everywhere

Block
Stop threats before connections are made

Consumer
SMB Connectivity
MSSP Enterprise
Protecting Network, Cloud, Device for 5G, IoT, Beyond

Secure Enterprise Mobility

Samsung and Cisco are partnering to provide the most secure mobile device platform with unmatched visibility for the enterprise.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Thank You
“There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.”

John Chambers