Healthcare Market Trends: Threat Centric Security for the Digital Age

Keval Shah,

Security Account Manager, Cisco Systems

kevshah@cisco.com

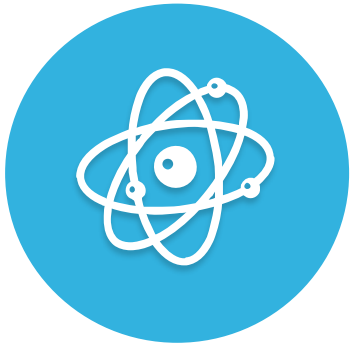
Why should we be concerned?

Industry (NAICS code)	Total	Small	Large
Agriculture (11)	1	1	-
Mining (21)	2	1	1
Utilities (22)	-	-	-
Construction (23)	1	1	-
Manufacturing (31–33)	11	2	5
Trade (42)	10	7	3
Retail (44–45)	43	15	17
Transportation (48–49)	8	2	4
Information (51)	2	-	-
Finance (52)	113	42	54
Real estate (53)	4	3	1
Professional (54)	35	18	-
Management (55)	-	-	-
Administrative (56)	24	14	5
Educational (61)	51	5	33
Healthcare (62)	1,403	573	339
Entertainment (71)	1	-	1
Accommodation (72)	3	1	1
Other services (81)	19	14	2
Public (92)	177	31	38
Unknown	23	-	-

Table 1.

Breaches by industry and organization size (where organization size is known)

Healthcare – Cyber Security Challenges



Digitization and Changing Business Models

Dynamic Threat Landscape

Complexity and Fragmentation

Talent Shortage

Complex Challenges for Healthcare Providers

BYOD

50%+

of hospitals are using smartphones or tablets

PHI Data Access

69%

of clinicians are using both a desktop/laptop and a smartphone/tablet to access data

Compliance

138%

the increase in HIPPA data breaches from 2012 to 2014

Breach

54%

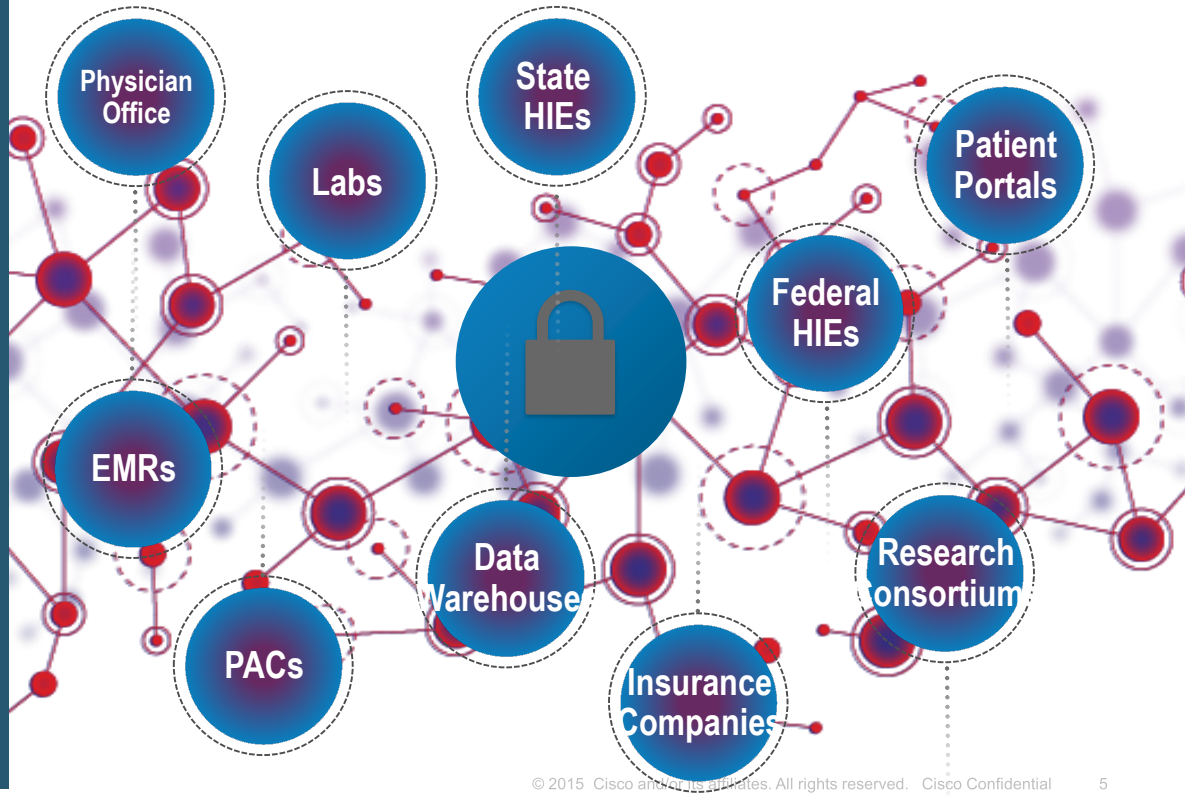
of breaches remain undiscovered for MONTHS

Security is *the* Top of Mind Concern

Source : Ponomen Research : June, 2015

Healthcare PHI & PII goes beyond 4 walls of the hospital

- Family physician
- Specialist clinic
- Blood Lab
- X-Ray / Cat Scan provider
- Local hospital
- Rehab facility after hospital discharge
- Online patient portals
- Insurance company (payer)
- Health Information Exchanges
- EMR-to-like-EMR integration
- Data Warehouse(s)
- Data push to patients & other providers
- Push to the State, research consortiums
- Data push of lab results to providers
- Data pull from EMRs for visiting patients



The Medical Device Challenge

- 20% growth per annum in number of medical devices
- No common standards or security
- Windows embedded 2009, (Windows XP)
- Dumb devices unable to support AV or End Point Protection
- Limited CPU and memory unable to sustain malware or DOS
- Half Life – Medical Devices last for up to 20 years
- Easiest way to infiltrate a healthcare network is via a medical device / medical device network – 802.11 40 bit WEP or RJ45 port
- Maximum patient harm can be an attack on a medical device

Top Challenges

1. Litigation – customers sue company – Multi-Billion $ Class Actions
2. Loss of Reputation as a result of a breach – lose customers
3. Fines for compliance failures – Industry Rules / National~ State Rules
4. Theft of balance sheets – WA hospital lost entire payroll
5. Loss of Intellectual Property – clinical research, formulations, test data
6. Loss of other non-public information – Board minutes, M&A, PHI, PII, PCI,
7. The hidden Gremlin - Industrial Control Systems (ICS) security – air, water, power, elevators

Limited Security Staff

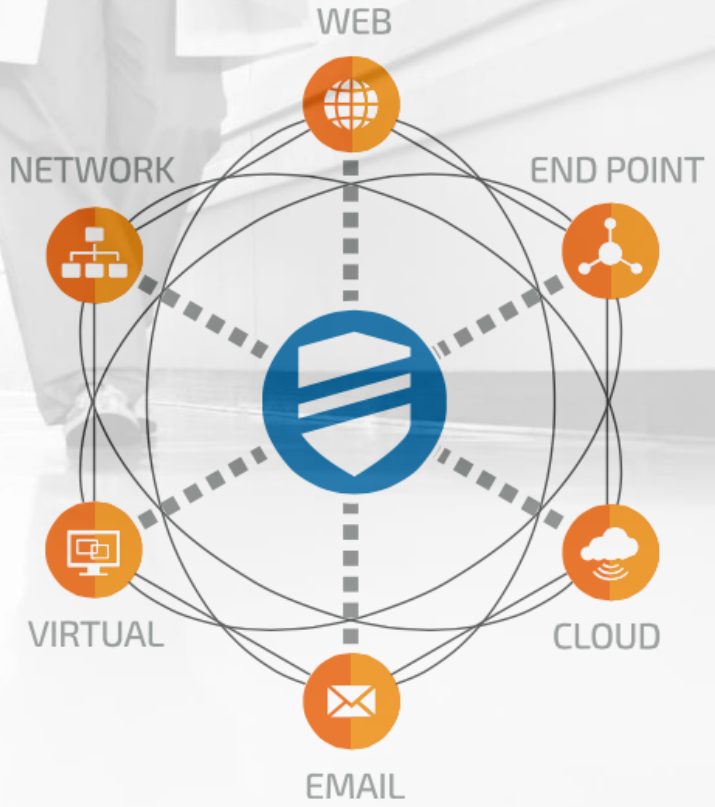
- 12x demand over supply for qualified experienced security professionals
- Lowest paid industries find it difficult to retain staff
- Staff too small to cover all aspects of security so focus on operations - leaving large gaps elsewhere

Distraction from Running the Business

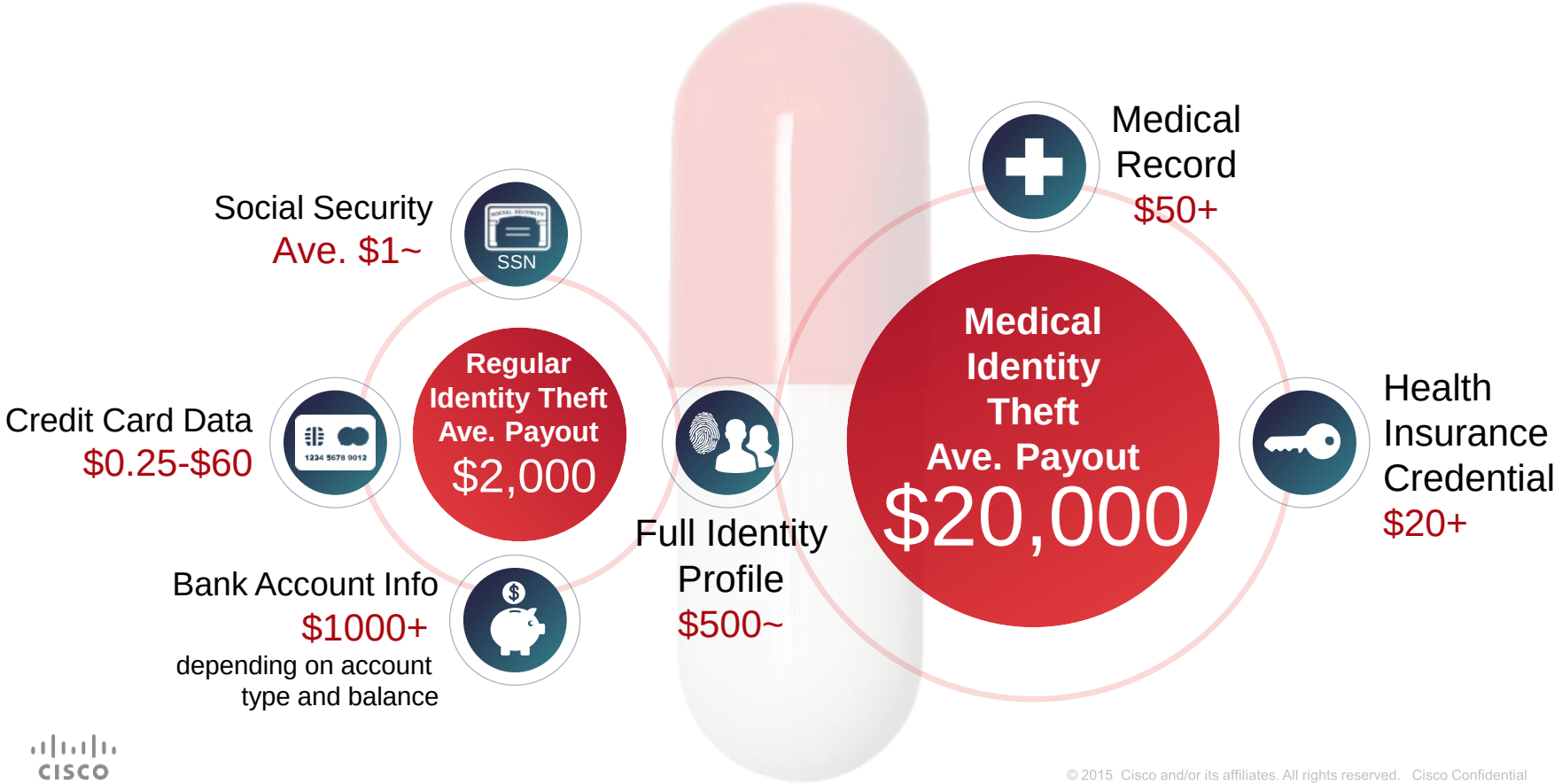
- Operational focus
- No time for higher value tasks or preparing for the future
- Need to outsource low value operations – “better, cheaper, faster”

Healthcare Specific Security Challenges

- Need to **ACCESS** information whenever and wherever by clinicians
- **AUTHENTICATION** to patient records must be **FAST**
- Movement towards **CLOUD APPLICATIONS** expands security risks
- Multitude of **MEDICAL DEVICES** – all connected and all must be secured (EKGs, Heart Monitors, Medicine Cabinets, implants, etc.)
- Use of **MOBILE DEVICES** and **BYOD** dissolves the network perimeter



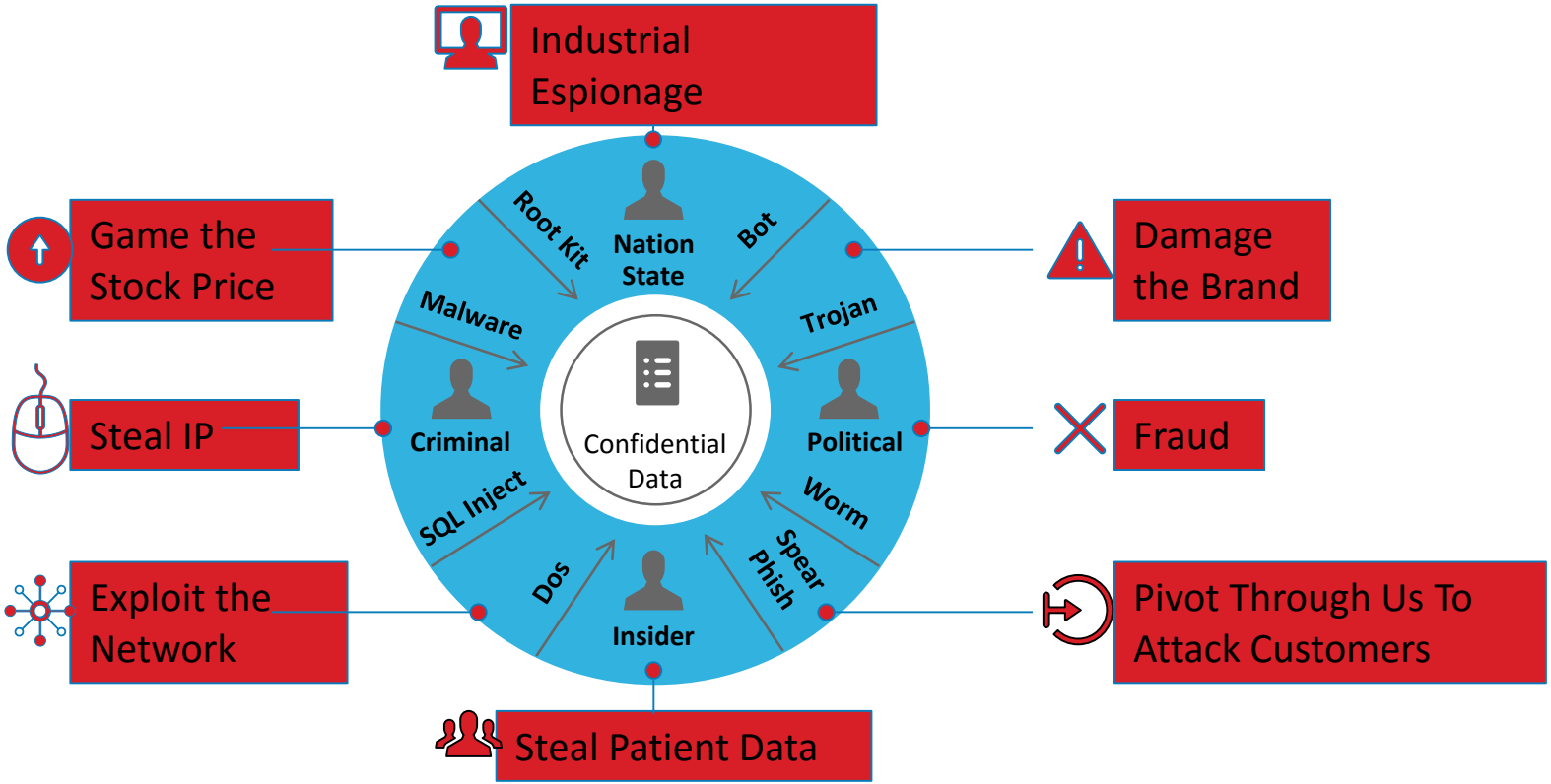
Motivated Threat Actors Behind Breaches:



Source: EMC

CIO / CISO 's End Game

Who, What, Where, When… HOW

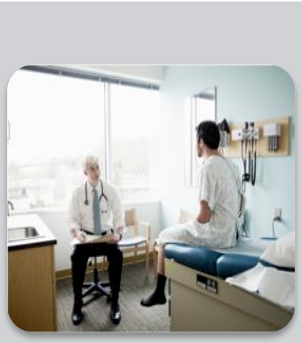


Cisco Confidential

Are you Ready?

Healthcare Security Scenarios

Today's Security Access Scenarios



Remote Physician Clinic

Clinician PHI Access

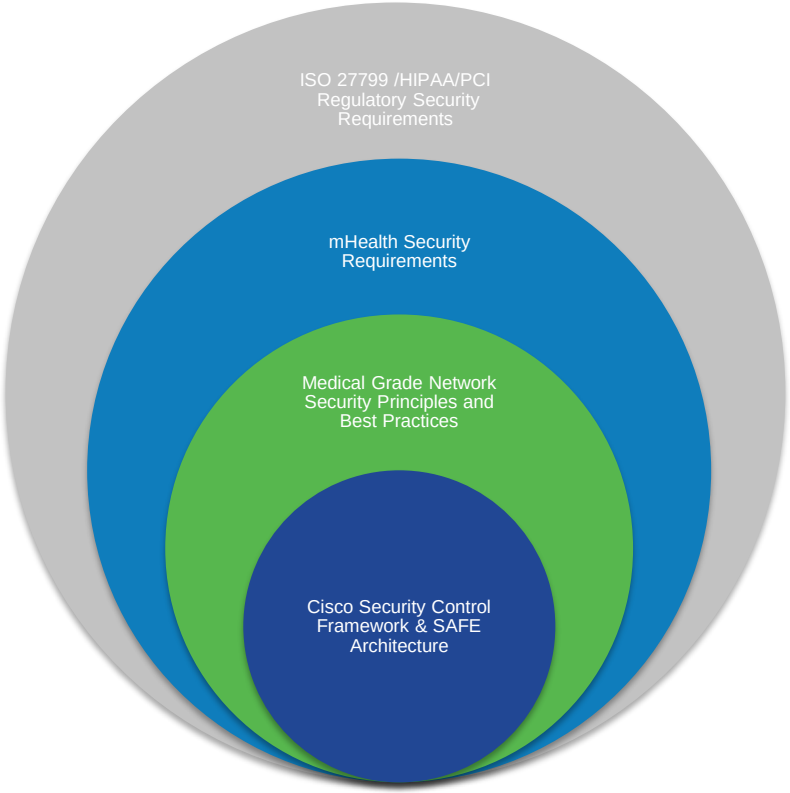
Bring Your Own Device Mobility/ Medical Devices

Patient Experience/Vendor Support/Guest Services

Virtual Physician

Connected Health Infrastructure– Security Architecture

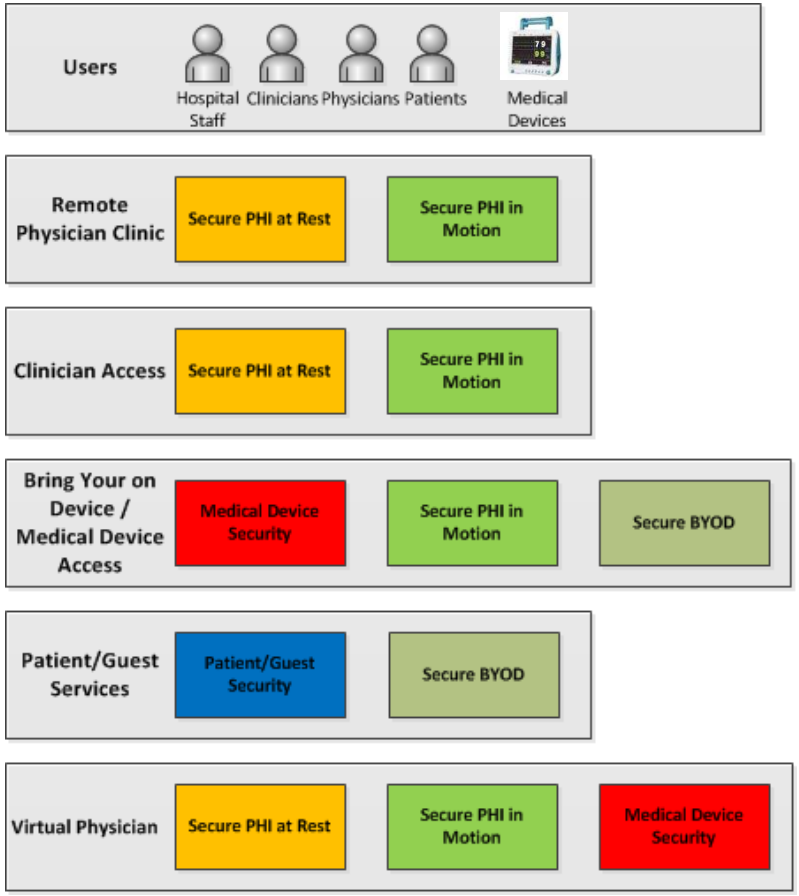
Cisco Connected Health Infrastructure Security Framework



Framework covers end to end security requirements for healthcare network to protect ePHI assets

MGN: Medical Grade Network is a set of Cisco recommended guidelines for building an optimal healthcare network

Securing the Healthcare Landscape



Security Capability to Solution Mapping

Business Imperatives

- Secure PHI at Rest
- Secure PHI in Motion
- Secure BYOD
- Medical Device Security
- Patient/Guest Security

Imperative	Solutions required to meet imperatives	Offers
	Advanced Threat Protection	1,2,3,4,5,6,7,8,9
	Network and Data Center Security	1,4,5,6,7,8,9,10,12,1314,15
	Secure Mobile and Endpoint Solutions	1,5,6,7,8,11,14,15
	Secure Content Gateway	1,2,3,11,12,13,14
	Access and Policy Management	1,2,4,5,7,8,14

Offers highlighted are comprised of multiple components from several solutions categories

Offers

1. Advanced Malware Protection (AMP)
2. AMP ThreatGrid
3. Cognitive Threat Analytics
4. Cyber Threat Defense
5. Next-Gen Firewalls
6. Next-Gen Intrusion Prevention
7. Software-Defined Segmentation (TrustSec)
8. Secure Access
9. Secure Data Center
10. Application Centric Infrastructure (ACI)
11. AnyConnect
12. Email Security
13. Web Security
14. Identity Services Engine
15. Wireless Intrusion Prevention

Cisco Security Solutions: http://www.cisco.com/c/en/us/products/security/solution-listing.html

Healthcare Security


Sourcefire Acquisition
AMP Everywhere OpenAppID
Managed Threat Defense
Cognitive Threat Analytics
NGFW
ThreatGrid
OpenDNS
PORTCULLIS
Lancope
NEOHAPSIS
Cisco Momentum in Security

Cisco Threat Intelligence - Unrevealed

100TB Security Intelligence	**150,000** Micro-applications	**5,500** IPS Signatures	**5B** Daily Email Connections
	93B Daily Email Messages	**150M** Deployed Endpoints	**1,000** Applications
13B Web Requests	**35%** Enterprise Email	**3-5 min** Updates	**4.5B** Daily Email Blocks
120K Sandbox Reports	**75,000** FireAMP Updates		**14M** Deployed Access Gateway

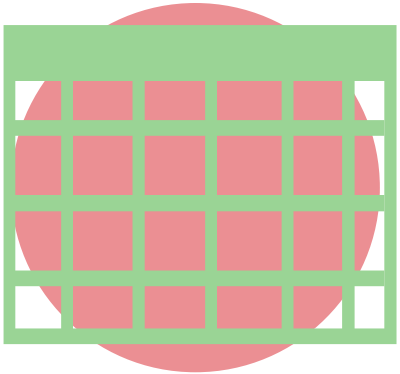
More Effective Against Sophisticated Attacks

Much Faster Than Most Organizations Discover Breaches

Industry

100

DAYS



vs.

Cisco

Less than

1 Day

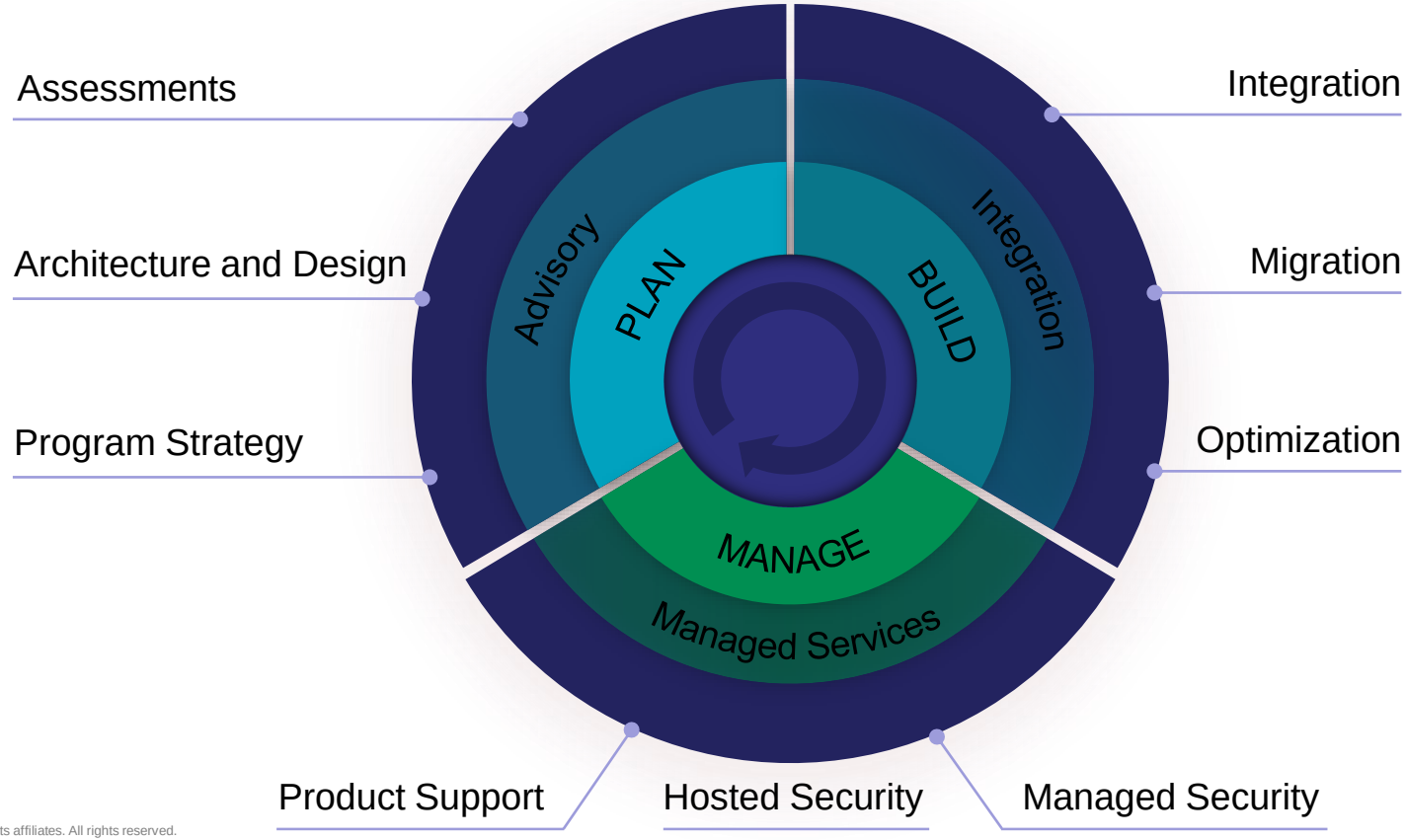
Source: Cisco Annual Security Report, 2016

Active Threat Analytics Security Operations Center

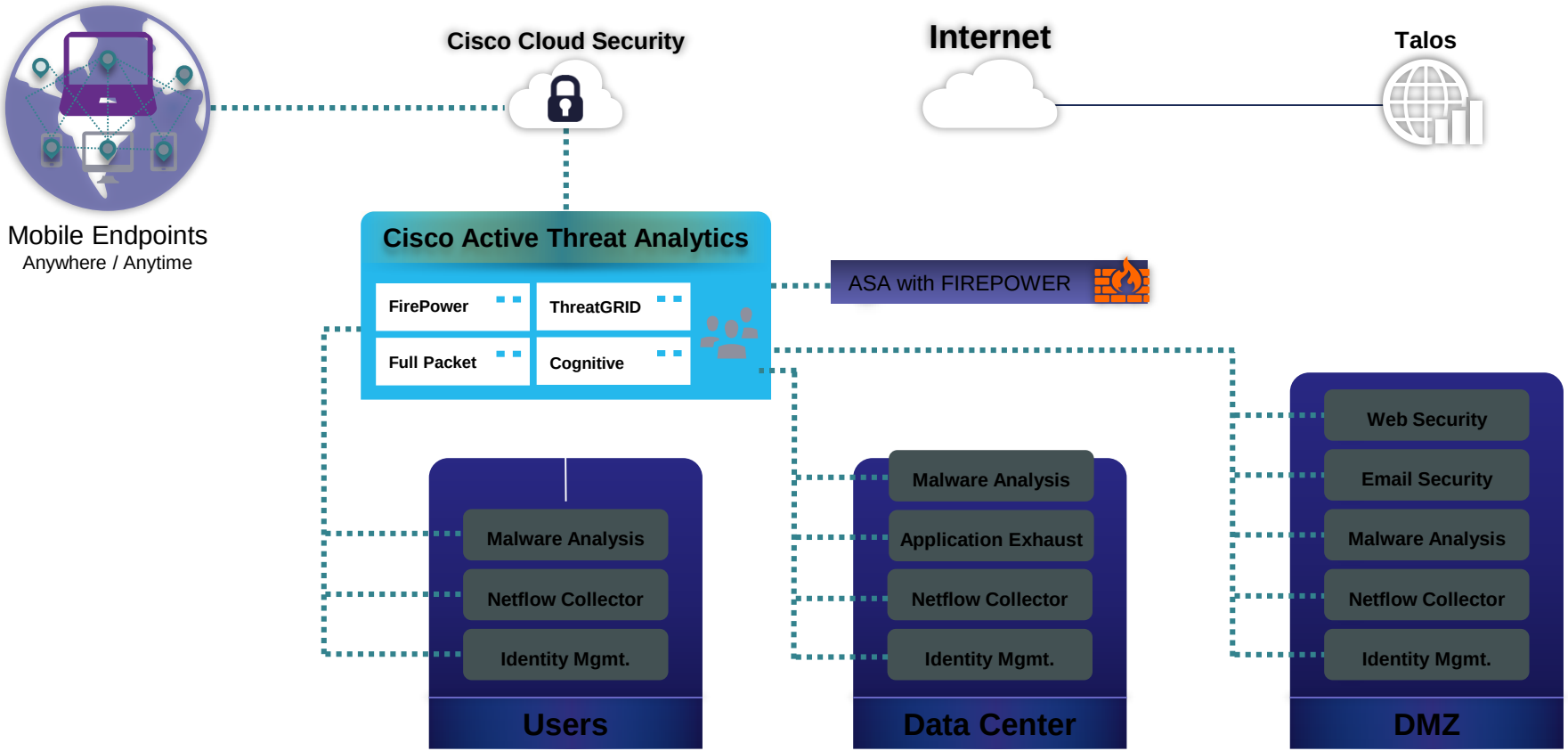
Complete Security Solutions

Accelerating to the Outcome

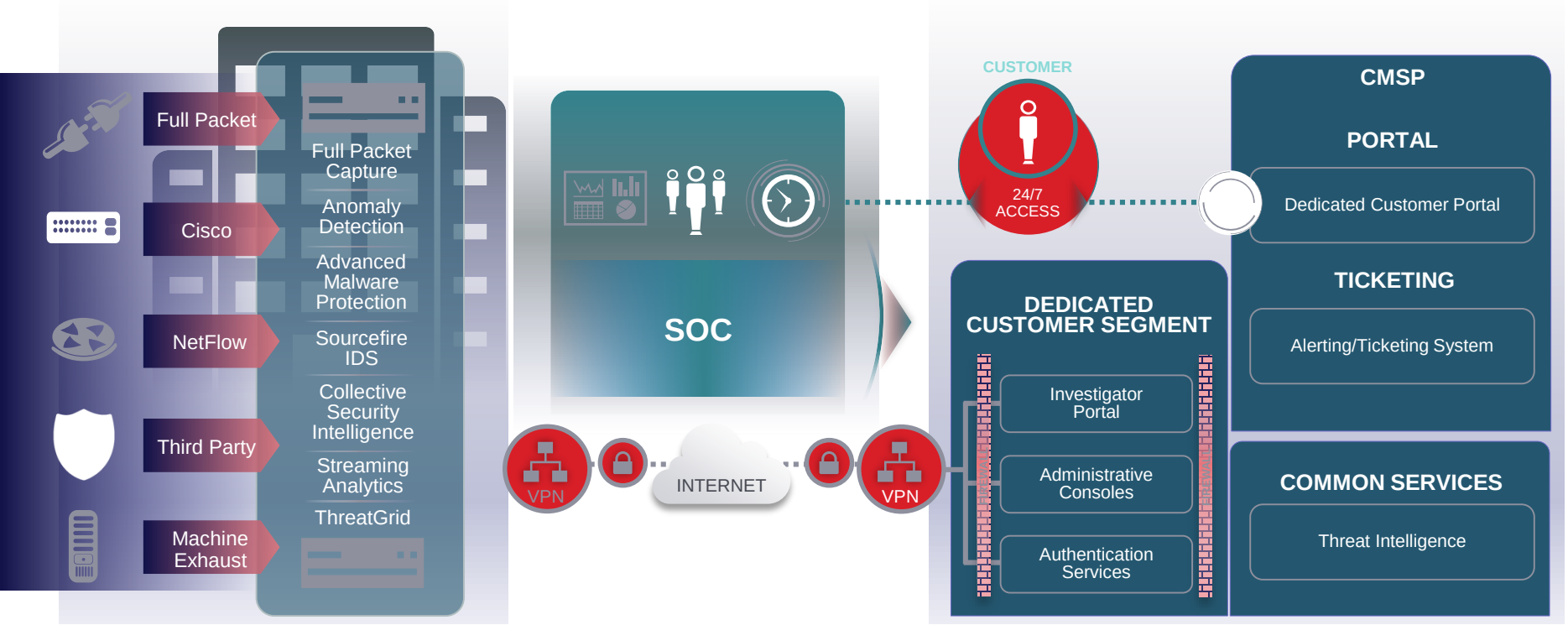
Integrating Services Support into the Lifecycle



ATA: A Comprehensive Threat Solution



Cisco Active Threat Analytics Premier



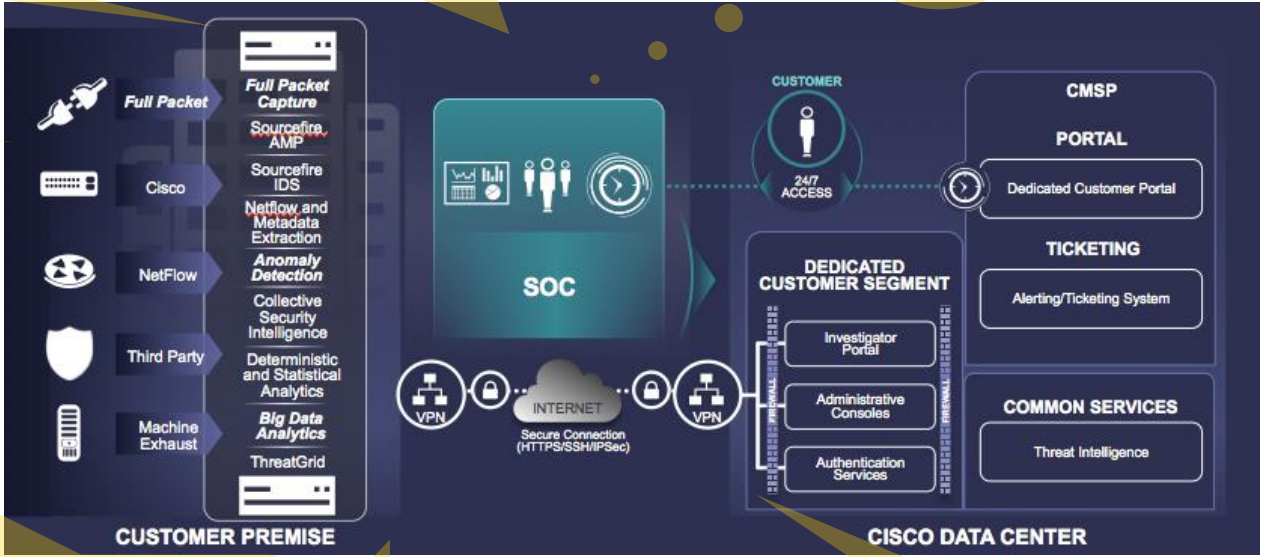
Analytics, Notification and Remediation Flow

ATA "kit" installed, owned and maintained by Cisco

Data from customer owned devices and ATA "kit" is monitored 24x7 by Cisco SOC via secure VPN

Talos
Cisco's threat intelligence organization is tightly aligned with our SOC

Customer owned security devices



Customer Operations Center

Threat Remediation may be handled by customer teams, by a managed service provider (such as Cisco ATA Essential), or by Cisco Incident Responders

Validated Threat and Remediation Requirements are communicated to Customer Operations Center in real time

Cisco Validates Threat

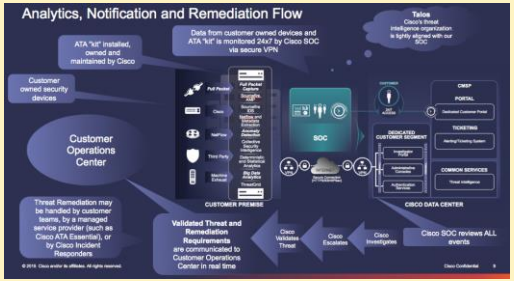
Cisco Escalates

Cisco Investigates

Cisco SOC reviews ALL events

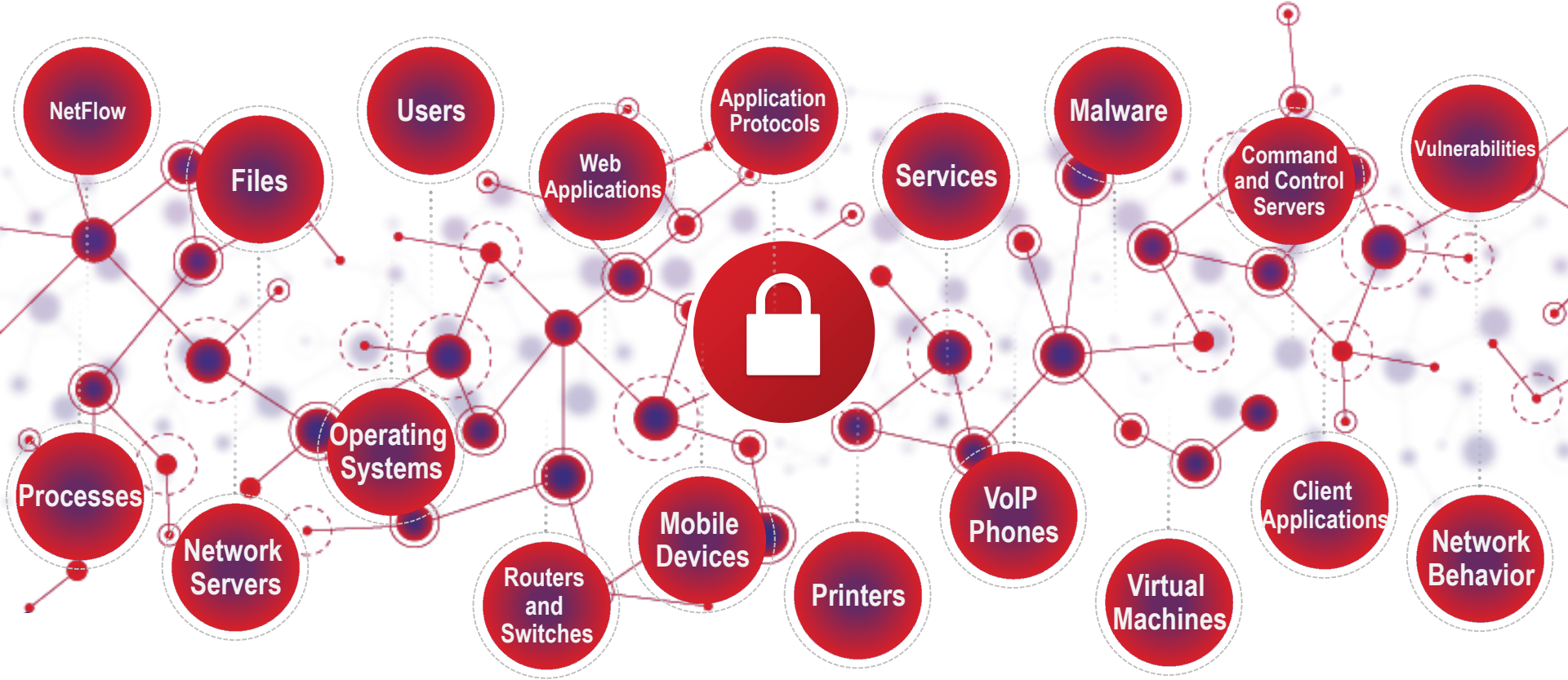
Healthcare Executive and Technical Leadership

Security Operational Staff



Cisco Advanced Services

Cisco Sees More To Protect Better



Summary