NACo Technology Innovation Summit

Making Cybersecurity Easier

Peter Romness
Cybersecurity Solutions Lead – US Public Sector
promness@cisco.com

Our Security Challenges

Changing Business Models

Dynamic Threat Landscape

Complexity and Fragmentation

Changing Business Models

Mobile

* Cisco IBSG, ** Cisco 2013 VNI, *** IDC

3.3 Devices Per Knowledge Worker*

55% IP Traffic Mobile by 2017**

Cloud

* Skyhigh Networks Industry Report, ** Cisco
*** Cisco VNI Global Mobile Data Traffic Forec

545 Cloud Aps Per Organization*

44% Annual Cloud Workload Growth ***

IoE

* Cisco IBSG, ** Cisco VNI: Global Mobile Data T
Forecast 2013-2018

50B Connected "Smart Objects" by 2020*

36X Growth in M2M IP Traffic 2013–18**

Security Implications

- No Clear Enterprise Edge
- Larger Attack Surface
- More Attack Vectors

Dynamic Threat Landscape

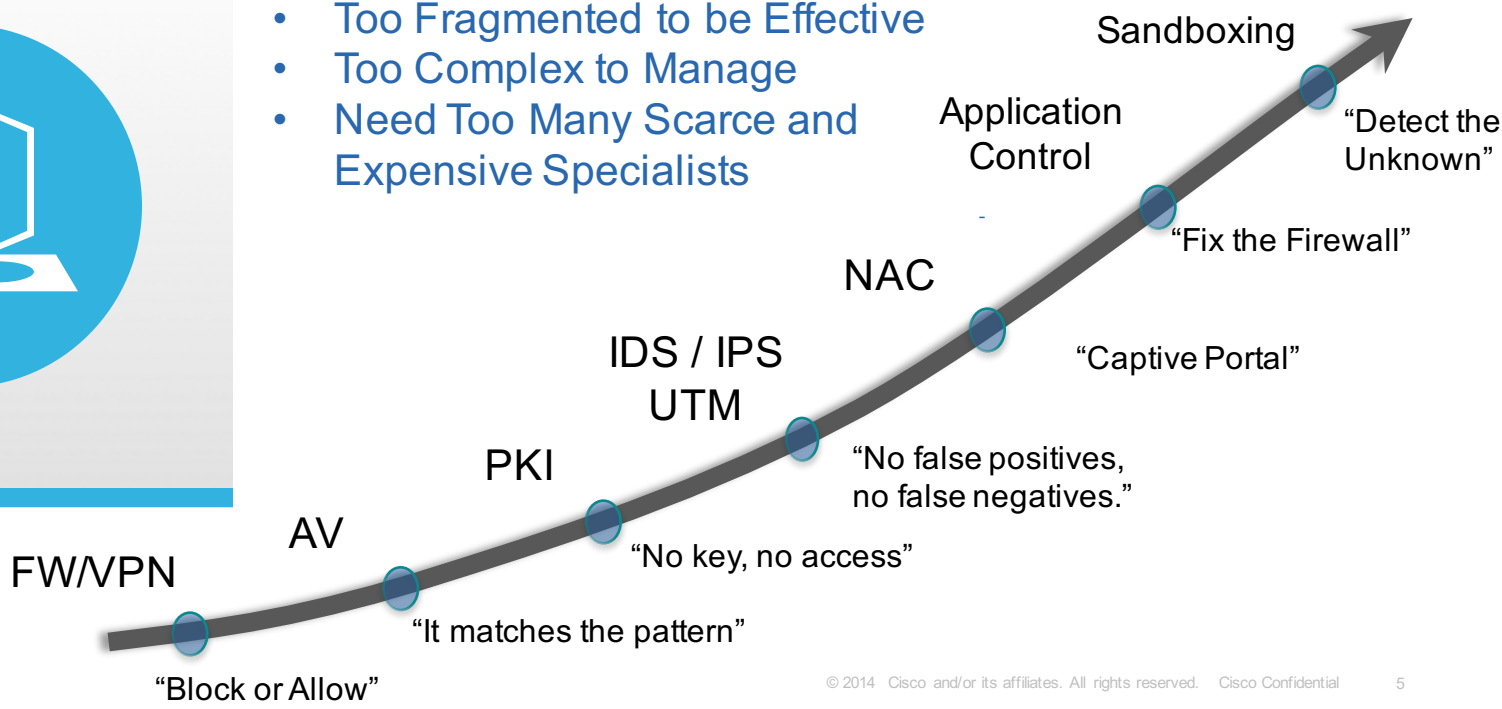
Security Implications

- Highly Motivated Attackers
- More Attacks
- More Likelihood of a Breach
- Hard for Defenders to Keep Up

Complexity and Fragmentation

Security Implications

- Too Fragmented to be Effective
- Too Complex to Manage
- Need Too Many Scarce and Expensive Specialists




Use Standards and Guidance
• NIST Framework
• CySafe
• NCCoE 1800 Documents
Automate Detection and Response as Much as Possible
Reduce Complexity
• Devices Working Together
• Fewer Platforms to Manage
Get Help
• Outsource Specific Functions
• Security as a Service
Making Cybersecurity Easier

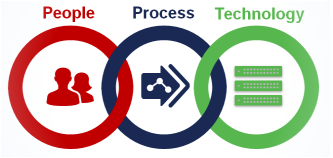
Using Standards

NIST Framework

Function		Category	
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

- Know what you have
- Secure what you have
- Spot threats quickly
- Take action immediately
- Restore operations

It's not all Technology



Function		Category		People	Process	Technology
ID	Identify	ID.AM	Asset Management	Applies	Applies	Applies
		ID.BE	Business Environment	Applies	Applies	
		ID.GV	Governance	Applies	Applies	
		ID.RA	Risk Assessment	Applies	Applies	Applies
		ID.RM	Risk Management Strategy	Applies	Applies	
PR	Protect	PR.AC	Access Control	Applies	Applies	Applies
		PR.AT	Awareness and Training	Applies	Applies	
		PR.DS	Data Security	Applies	Applies	Applies
		PR.IP	Information Protection Processes and Procedures	Applies	Applies	Applies
		PR.MA	Maintenance	Applies	Applies	Applies
		PR.PT	Protective Technology	Applies	Applies	Applies
DE	Detect	DE.AE	Anomalies and Events	Applies	Applies	Applies
		DE.CM	Security Continuous Monitoring	Applies	Applies	Applies
		DE.DP	Detection Processes	Applies	Applies	
RS	Respond	RS.RP	Response Planning	Applies	Applies	
		RS.CO	Communications	Applies	Applies	
		RS.AN	Analysis	Applies	Applies	Applies
		RS.MI	Mitigation	Applies	Applies	Applies
		RS.IM	Improvements	Applies	Applies	
RC	Recover	RC.RP	Recovery Planning	Applies	Applies	
		RC.IM	Improvements	Applies	Applies	
		RC.CO	Communications	Applies	Applies	

- **Only half** of the Framework's Categories are addressed by **technology**
- Highlights the importance of both **people and process** in cybersecurity

Reduce Complexity

Reduced complexity provides better detection and reduced cost with fewer platforms to manage and support.

- Agile and Open Platforms
- Build for Scale
- Consistent Control, Management

- Reduce information overload
- Focus security staff on high value activities
- Save time and money!

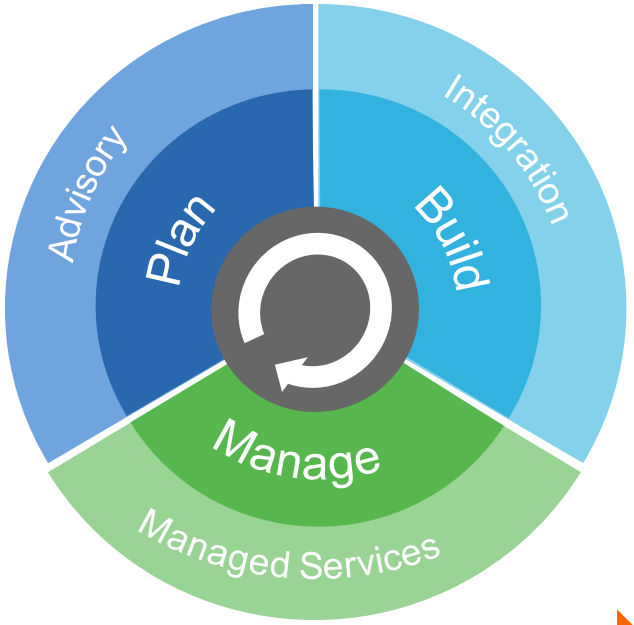
Automate Detection and Response

Ability to automatically take action on common threats based upon user determined policy

- Block, drop, quarantine
- Prioritize actions needed
- Customization

- Allows faster response
- Focus security staff on high value activities
- Save time and money!

Get Help - Outsourcing



Outside resources either onsite or offsite to fulfill specific capabilities

- Onsite staff to fill vacancies
- Cloud based applications
- Onsite equipment managed from cloud

- Access to needed capabilities
- Economies of scale
- Focus security staff on high value activities
- Save time and money!

Network as a Sensor
Network as an Enforcer

Network as a Sensor

- Detect Rich Endpoint Data
- Detect Anomalous Flows
- Detect User Access Policy Violations

Network as an Enforcer

- Segment the Network to Contain Attacks
- Enforce Policy to Protect Applications and Data
- Automate Security Operations

Most organizations have much of this capability already in their network

Cisco's Approach

Visibility-Driven

Network-Integrated,
Broad Sensor Base,
Context and Automation

See and Stop Threats before they do damage

Threat-Focused

Continuous Advanced Threat Protection, Cloud-Based Security Intelligence

Find Threats Wherever they Are

Platform-Based

Agile and Open Platforms,
Built for Scale, Consistent Control,
Management

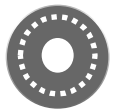
Save Money & Time with Reduced Complexity & Automation

Resources to Help Customers be Successful

Network

Endpoint

Mobile



Virtual

Cloud

TOMORROW starts here.