Using Zero Trust, CARTA, NIST, Federal CDM and Others to Inform a

Cybersecurity Best Practices Approach

Peter Romness
Cybersecurity Solutions Lead – US Public Sector CTO Office

October 2019

Attack landscape constantly evolving

Advanced Persistent Threats

Supply chain attacks

Ransomware

Unpatched Software

Data/IP Theft

Spyware/Malware

Malvertising

Wiper Attacks

Drive by Downloads

Phishing

Rogue Software

Man in the Middle

Botnets

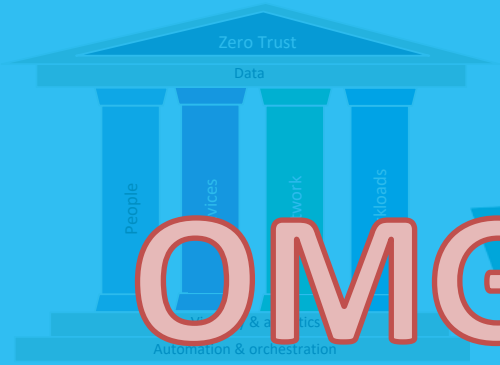
DDoS

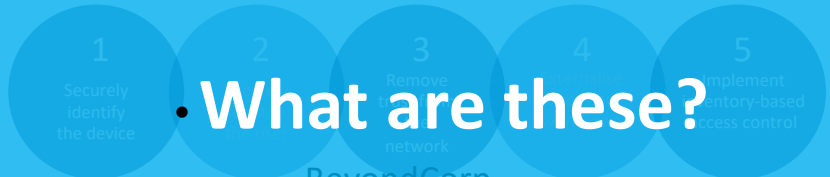
Credential compromise

Cryptomining


Impossibly complex
Network & Infrastructure Security
Advanced Threat Protection
NAC
SDN
DDoS Protection
DNS Security
Network Analysis & Forensics
Network Firewall
Deception
Web Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Other
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Security Ratings
Pen Testing & Breach Simulation
GRC
Security Awareness & Training
Security Ops & Incident Response
SIEM
Security Incident Response
Security Analytics
Momentum
Threat Intelligence
IoT
IoT Devices
Connected Home
Messaging Security
Digital Risk Management
Security Consulting
Blockchain
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Fraud & Transaction Security
Cloud Security
Container
Infrastructure
CASB

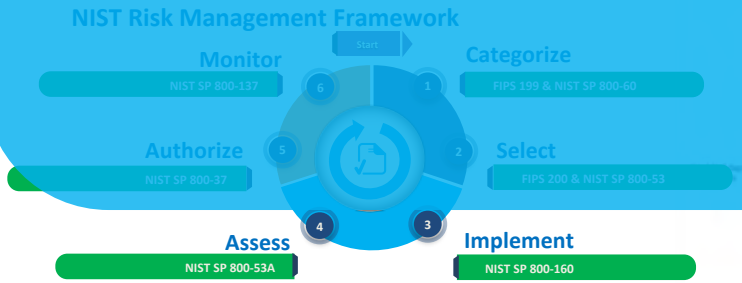
Approaches and Frameworks





OMG

- What are these?
- Why are we hearing about them?
- How can I address them?



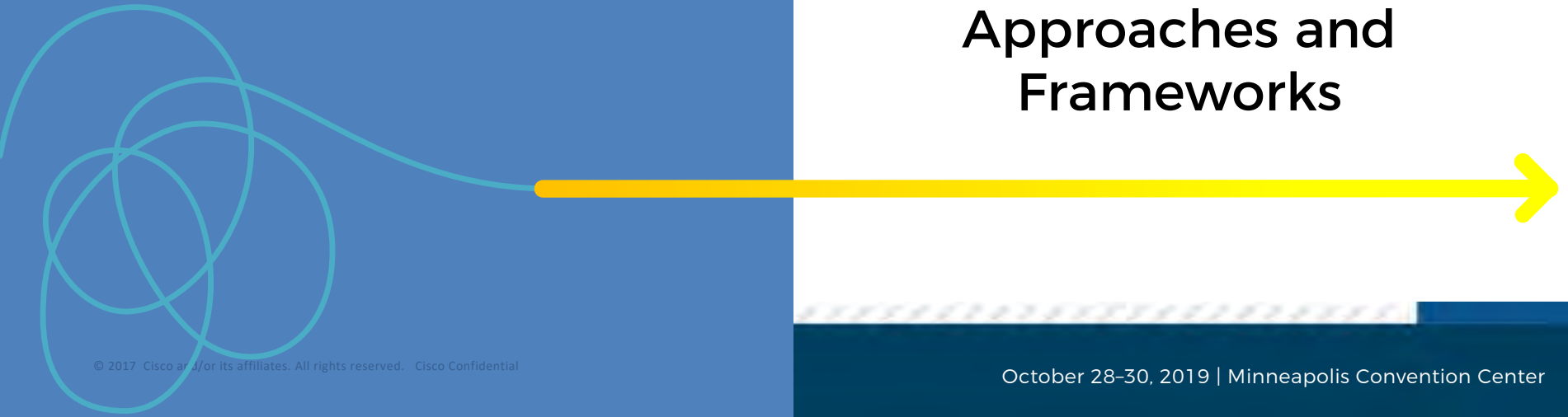
CJIS

CDM

CARTA

Let's go

from Overwhelmed to Empowered



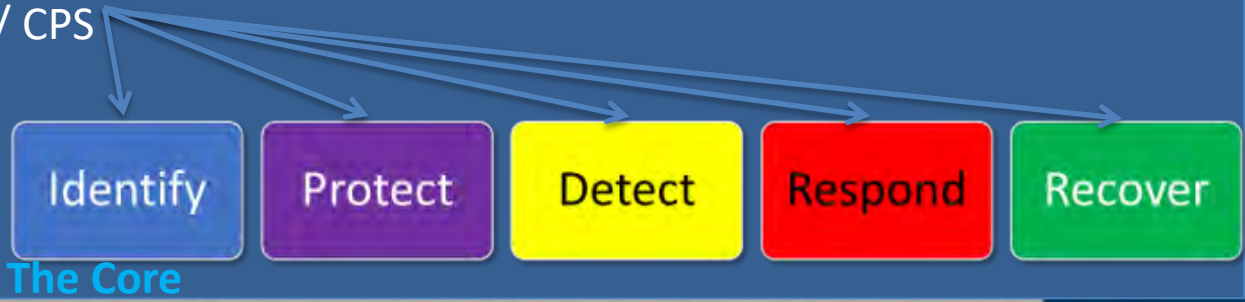
If you have a scalable, open and automated foundation, you can address all Approaches and Frameworks

The NIST CyberSecurity Framework

NIST CSF enables more effective management of risk

- **What:** Prioritized, flexible, repeatable, performance-based, cost-effective approach – becoming a de-facto standard
- **Goal:** A common language to identify, assess and manage cyber risks
- **Business drivers:** guide cyber resources and activities to help manage risk
- **3 parts:** Framework Core/ 4 Maturity Tiers / Your Profile
  - Core alignment with business requirements, risk tolerance and organizational resources
- **Adaptable** to IT / IoT / ICS / CPS

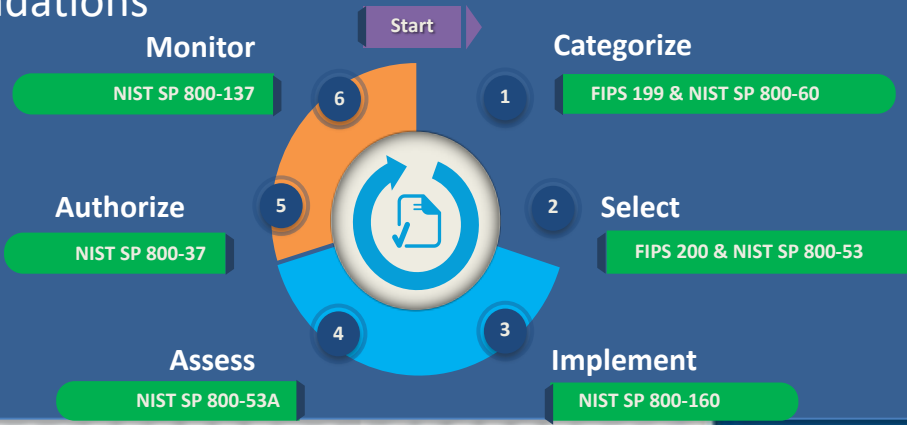
It's FLEXIBLE…
and it's NOT a Checklist!!!



The NIST Risk Management Framework (RMF)

NIST RMF is a process flow and more detailed reference then CSF

- **What:** A more prescriptive Risk Management Process.
- **Goal:** Describes more detailed "Outcomes" then CSF. It is a great reference
- **Process:** Uses NIST 800 series Special Publications for each part of the risk management cycle
- **Business drivers:** Still flexible, still recommendations
  – but more detail to drive decisions
- **Adaptable to:** All environments



It's still FLEXIBLE…
But is kind of a Checklist

Source: NIST RMF Overview, http://csrc.nist.gov/groups/SMA/fisma/framework.html

DoD RMF

Driving the Department of Defense to risk based threat management

- **What:** A DoD implementation of NIST RMF
- **Goal:** Establish and use of an integrated enterprise-wide decision structure for cybersecurity risk management. Move the DoD from STIG to Risk Management
- **Process:** References NIST 800 series Special Publications for the DoD specific environment
- **Encourages:** Reciprocal acceptance of DoD and other federal agency authorizations
- **Included in:** All acquisition processes

DoD Goal: Less checklist…
More risk based decisions

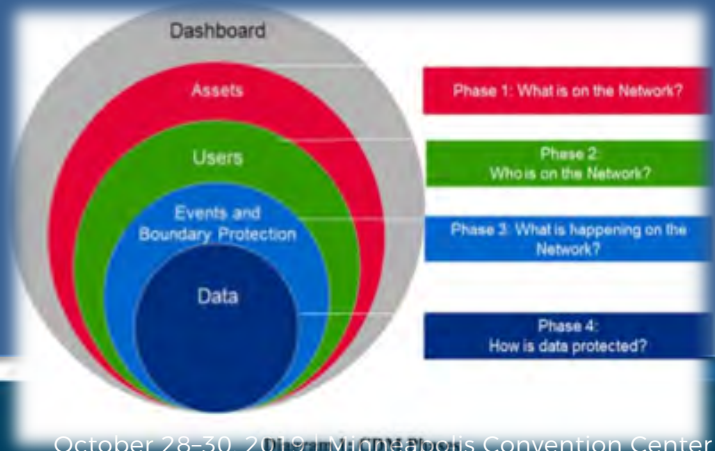
Continuous Diagnostics & Mitigation (CDM)

Federal requirement for Federal Civilian Agencies

- **What:** Federal mandate to protect and continuously monitor civilian sector federal departments and agencies
- **Who:** Managed by DHS – Administered by GSA - Enforced by OMB
- **Goal:** Threat protection and continuous reporting of Assets, Users, Data, Events
- **Process:** Required **h**ierarchal dashboard
  Department→Agency→OMB
- **Mandate:** Holds agency heads responsible with report cards and budget withholding compliance

Federal Requirement…

Mostly about compliance and reporting



Criminal Justice Information System (CJIS)

FBI Requirement to connect to the CJIS database

- **What:** Requires compliance to access CJIS Data
- **Who:** Every law enforcement agency in the nation who uses FBI criminal justice information to reduce and stop crime
- **Audits:** Audits occur every three years, and non-compliance has serious ramifications – including potential loss of access to FBI CJIS systems
- **Based on:** NIST RMF particularly NIST SP800-53 compliance

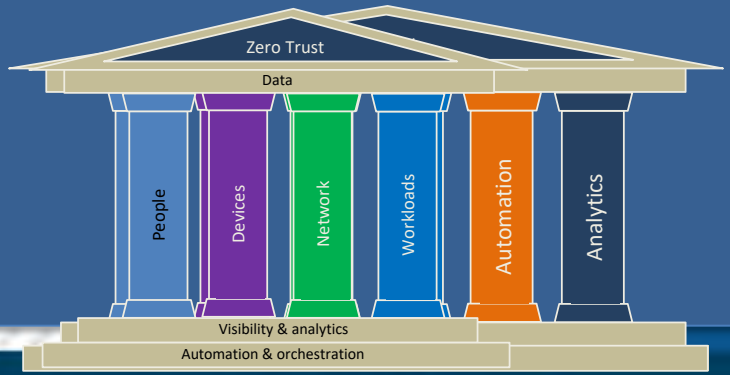
FBI Requirement…

Completely about compliance

Zero Trust
Popularized by Forrester - ZT and ZTX

- **What:** A security strategy based on “least-privilege” to address the modern “perimeter-less” IT environment
- **Intent:** Assumes all environments are hostile - no access until proven trusted
- **Tenants:** All users, devices, applications, data, and network flows encrypted, authenticated and authorized
- **Enablement:** Visibility and automation systems are what allow a zero trust network to be built and operated
- **Adaptable to:** All environments
- **Missing:** Threats

Zero Trust is a strategy and design approach
- not a checklist or a thing you buy



BeyondCorp

Google's model implementation of Zero Trust

- **What:** **C**loud focused - models a high level guide to implementing their Zero Trust implementation
- **Intent:** **S**hift access controls from the perimeter to individual devices and users
- **Process:** Identify devices and users, remove trust, externalize apps and workflows, implement access control
- **Tenants:** Perimeterless design, context aware, dynamic access controls

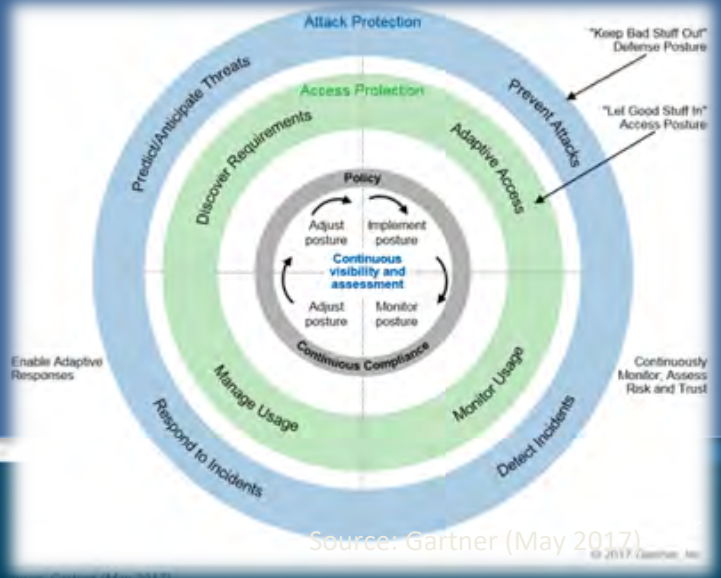
BeyondCorp is a Zero Trust example
- It can be used as a guide

CARTA - Continuous Adaptive Risk and Trust Assessment

Gartner's more comprehensive response to Zero Trust

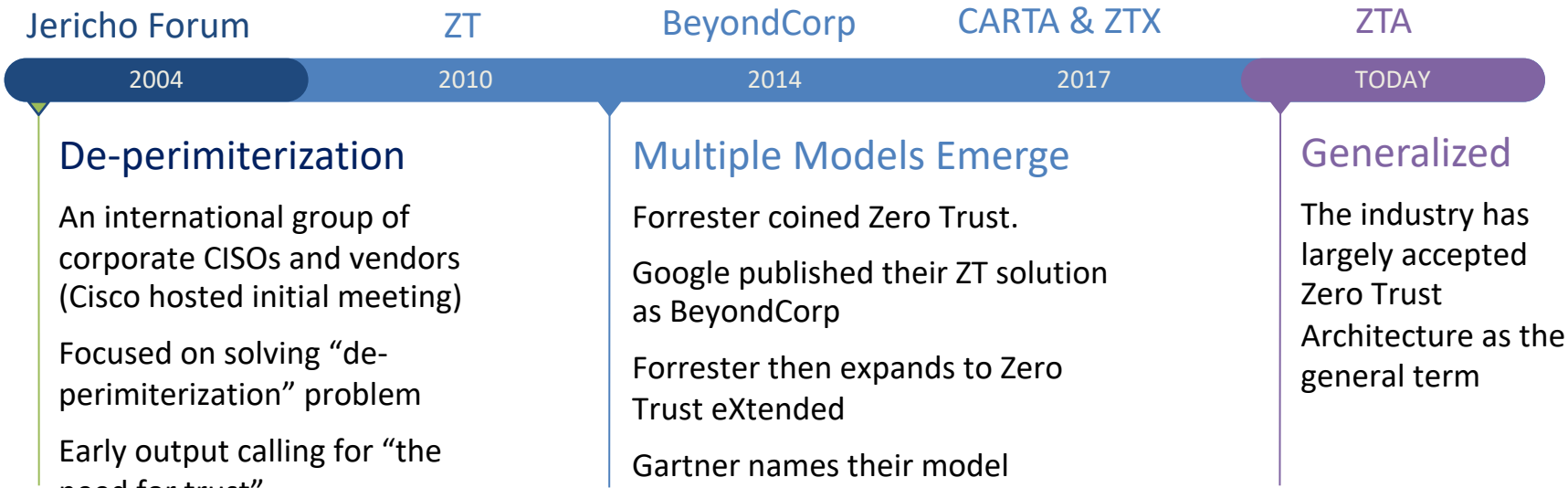
- **What:** Similar to Zero Trust with more emphasis on Threat protection
- **Intent:** Virtuous cycles for: Access Protection
  Threat Protection
  Implement → Operate/Monitor → Analyze → Adjust
- **Applies to:** All users, systems, system activities, payloads, networks
- **Enablement:** Emphasizes continuous improvement

CARTA is a strategy and design approach -
not a checklist or a thing you buy



Source: Gartner (May 2017)

A little bit of Zero Trust history



Zero Trust

- Zero Trust is not a bolt-on security product – must be designed into the network
  - Essential with impending devices/sensors/data explosion
- No implicit trust
  - Must authenticate before being allowed to connect to any asset on the network
  - Assume all traffic, regardless of location, is a potential threat
- Provide total visibility and analytics across the entire network
  - Continuously monitor/inspect/log all traffic, assess threat and automate responses
  - Detect and respond to anomalous activity in real-time
- Ensure granular network segmentation by user, device and application
  - Adopt a least-privileged strategy – only grant access to needed resources to perform their job
- Open, extensible Foundational platform that works with existing investments
- Optimize risk management through real-time response to dynamic threats

Security approach to confront risk

Continuously detecting threats and verifying trust

Continuous threat detection

Prevent attacks while continuously detecting and remediating the most advanced threats

Continuous trust verification

Continuously verify identity and device trust across the software-defined perimeter

Cisco Zero Trust Recommendations

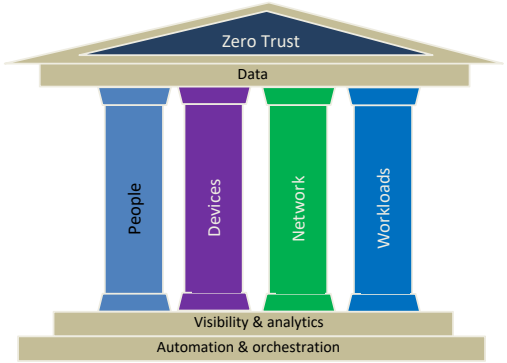
Trusted Workforce
User and Device Access

Trusted Workplace
IoT, Edge and Sensor Access

Trusted Workloads
App and Data Access

Threat Intelligence and proactive threat defense

How can I address these?



BeyondCorp

HIPAA
Health Insurance Portability & Accountability Act

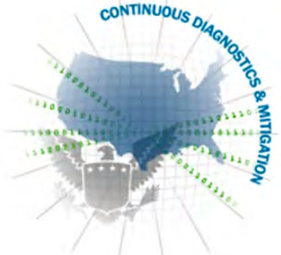
PCI

NIST Cybersecurity Framework

NIST Risk Management Framework

CARTA

CJIS



CDM

Need Best of Breed, Integrated Environment

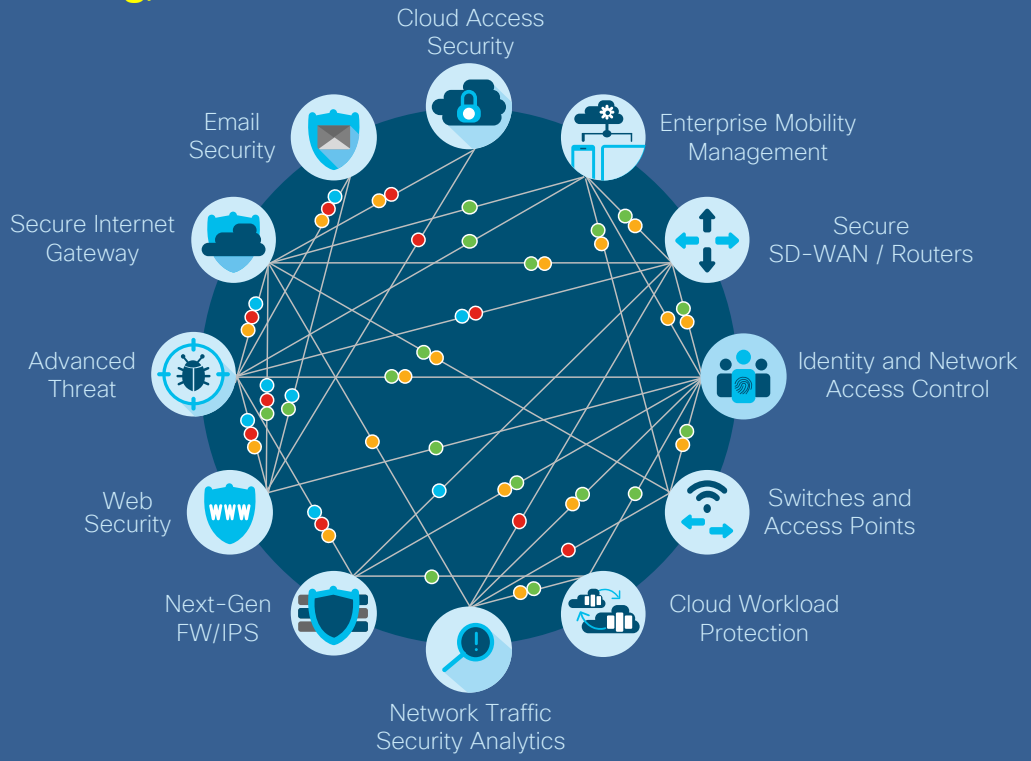
With Cross-domain Analytics, Information Sharing, and Automation

Threat Intel/Enforcement
Increased Threat Prevention

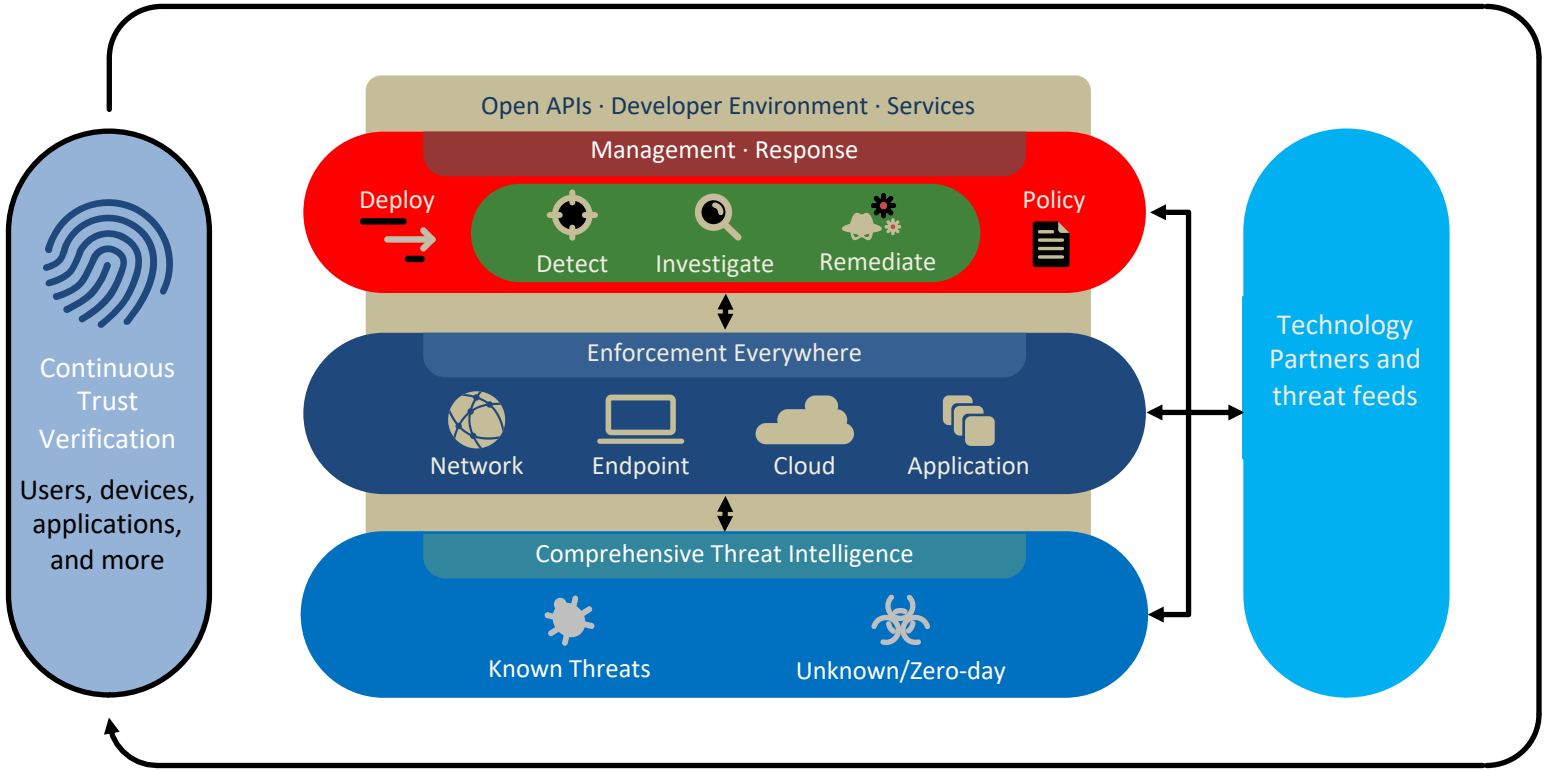
Event Visibility
Decreased Time to Detect

Context Awareness
Decreased Time to Investigate

Automated Policy
Decreased Time to Remediate



Modern Security Architecture



Steps to a Zero Trust architectural approach
A journey with granular-enforcement based on context

Establish Trust Level

Establish SD-Perimeter

Manage Risk Level

1 User-Device Trust

2 IoT Trust — AND/OR — Workload Trust

Inventory · Assess
Authenticate · Authorize

3 App and Data Access

4 Network Access

Authorized SD-Access
Micro-Segmentation

5 Policy Normalization

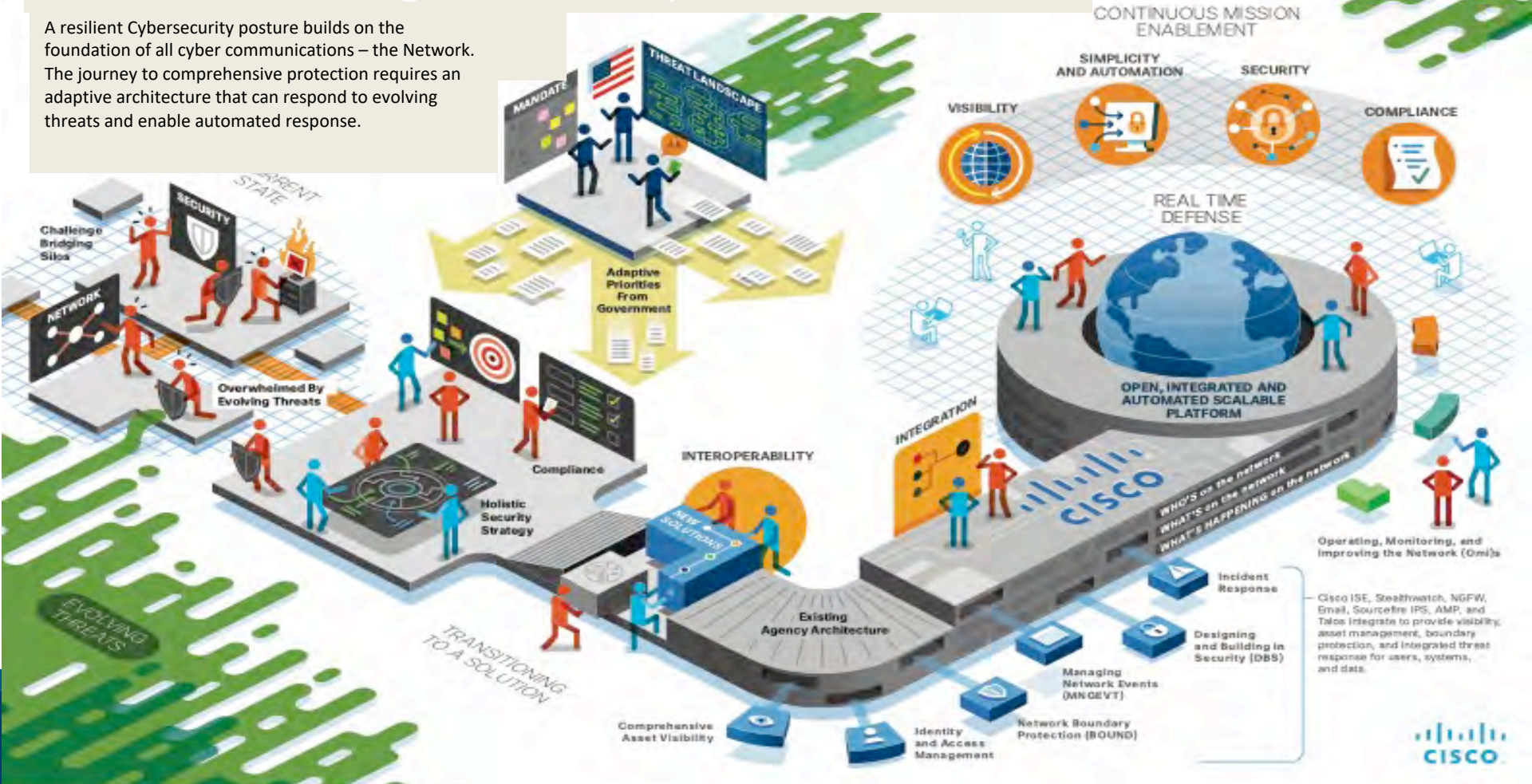
6 Threat Response

Continuous Detection and Verification

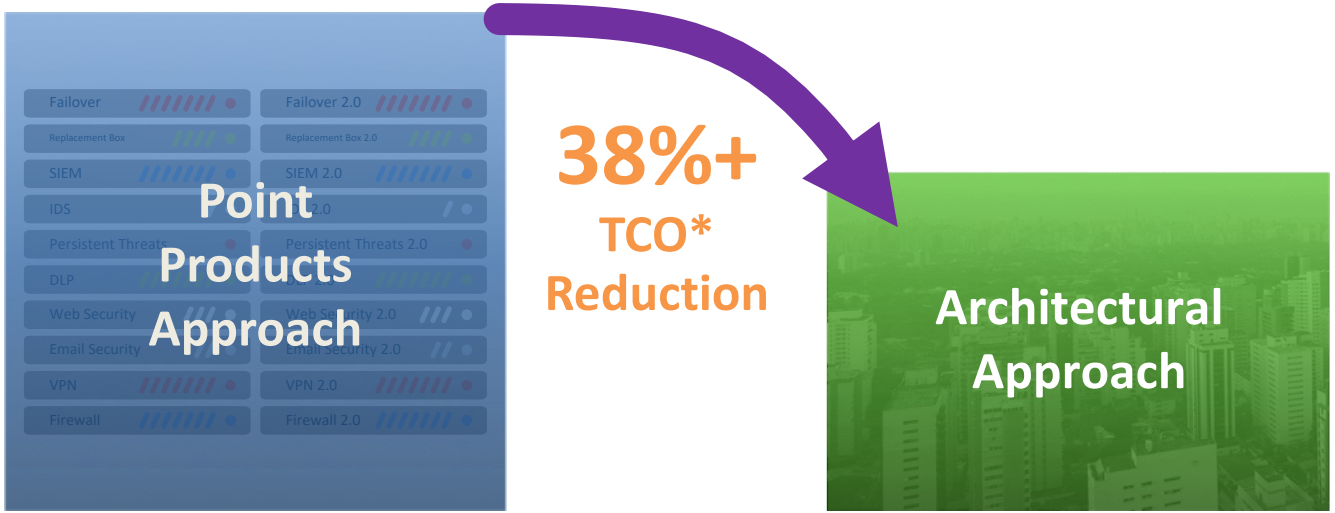
Shift from macro - binary to micro - contextual

The Path to an Integrated Security Platform

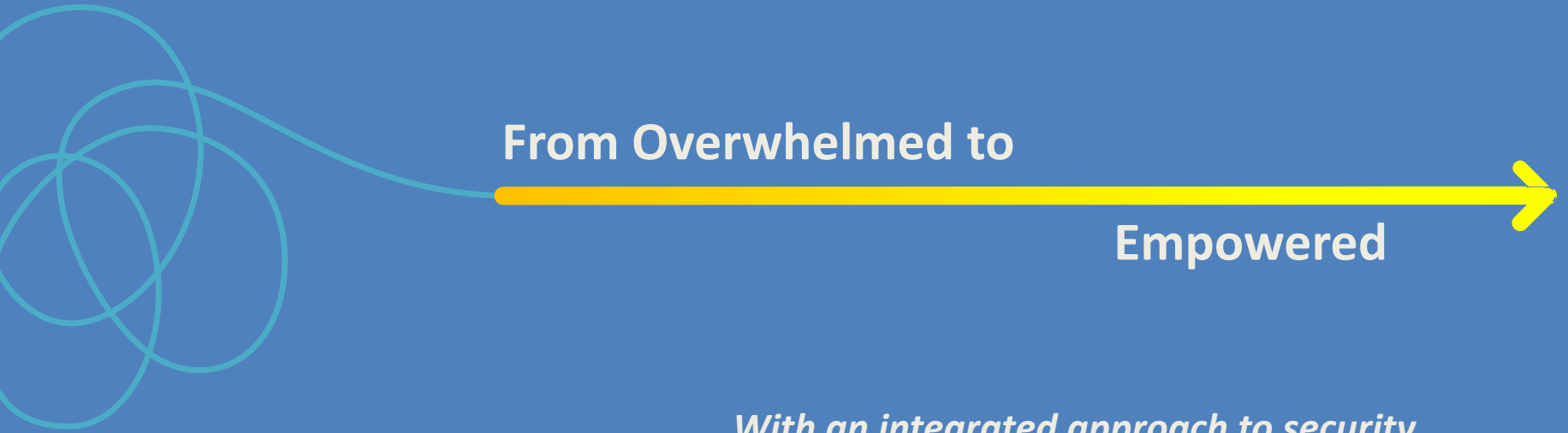
A resilient Cybersecurity posture builds on the foundation of all cyber communications – the Network. The journey to comprehensive protection requires an adaptive architecture that can respond to evolving threats and enable automated response.



An integrated threat defense also saves money



FORRESTER



With an integrated approach to security

If you have a **scalable, open** and **automated** foundation, you can address all Approaches and Frameworks

Cisco products to meet:

ZT, ZTX and CARTA

Identity Services Engine	SDA, policy enforcement, micro-segmentation, endpoint profiling & posture
AMP Everywhere	Advanced Malware Protection
StealthWatch	Traffic Analysis – Identify abnormal and known-bad traffic patterns
Tetration	Data Center Policy, Application, policy and traffic analysis
Cloudlock	Security for SAAS applications
Cisco DNA-Center	Campus Segmentation w/ SDA
APIC	Data center policy, ACI
AnyConnect	Posture, dot1x, EAP-Chaining, MACsec, Umbrella, NVM
ThreatGrid	Threat research and response – endpoint security
Encrypted Traffic Analytics	Malware detection in encrypted traffic without decryption
Duo	Application access control with multi-factor authentication (MfA)

Continuous Diagnostics Mitigation (CDM)

CDM Phase		Phase 1 – What is on the Network?				Phase 2 – Who is on the Network?				Phase 3 – How is the Network protected?	Phase 3 – What is happening on the Network?			Form Factor
Cisco Products		Hardware Asset Management	Software Asset Management	Configuration Settings Management	Vulnerability Management	Manage Trust	Manage Behavior	Manage Credentials	Manage Privileges	Boundary Protection	Manage Events	Operate, Monitor and Improve	Design and Build-in Security	
Network Security Products	Route / Switch (LAN)				✓	✓	✓	✓	✓	●			●	P
	SD - WAN				✓	✓	✓	✓	✓	●			●	P / V
	ESA / WSA		✓	✓	✓	✓	●	✓	✓	●		●	●	P / V
	FTD / NGFW / NGIPS	●	✓		●	●	●	●		●	✓	●	✓	P / V / C
	ISE / TrustSec	●	●	✓	●	●	✓	●	●	●	✓	●	✓	P / V
	SW	✓	✓	✓	●	✓	●	✓	✓	✓	✓		●	P / V / C
	AMP / TG		✓		●	✓	●		✓	●		✓	✓	P / S / C
	Meraki	●	●	✓	●	●	✓	●	●	●	✓	●	✓	P / C
	AC	●	✓		✓	●		●	✓	●		●	✓	S
	Umbrella		✓	✓	✓		●		✓	●	✓	●	●	C
	Cloudlock				✓	●			●	●	✓		●	C
	ETA		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	C
Management	FMC / PI / DNA Center		✓	●	✓	●	●	●	●	●	✓	●	●	P / V / S
	pxGrid	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	S
Threat Intelligence	CTA		✓	✓	✓	●		✓	✓	✓	✓		●	C
	Talos		✓	✓	✓	✓	●	✓	✓	✓	✓		●	C

● Primary ✓ Secondary

Abbreviations

- **FTD** – Firepower Threat Defense
- **NGFW** – Next-Generation Firewall
- **NGIPS** – Next-Generation Intrution Prevention System
- **FMC** – Firepower Management Center
- **PI** – Prime Infrastructure
- **DNA Center** – Digital Network Architecture Center
- **ESA** – Email Security Appliance
- **WSA** – Web Security Appliance
- **AMP / TG** – Advanced Malware Protection / Threatgrid
- **ISE / TrustSec** – Identity Services Engine / TrustSec
- **ETA** – Encrypted Traffic Analysis
- **CTA** – Cognitive Threat Analytics
- **Form Factor** – Physical (**P**)– device comes in its own server format/appliance
- **Form Factor** – Virtual (**V**) – device runs as a Virtual Machine on a hypervisor
- **Form Factor** – Software (**S**) – device is installed as software/agent
- **Form Factor** – Cloud (**C**) – device runs in cloud services (For example, AWS, Azure, etc.)

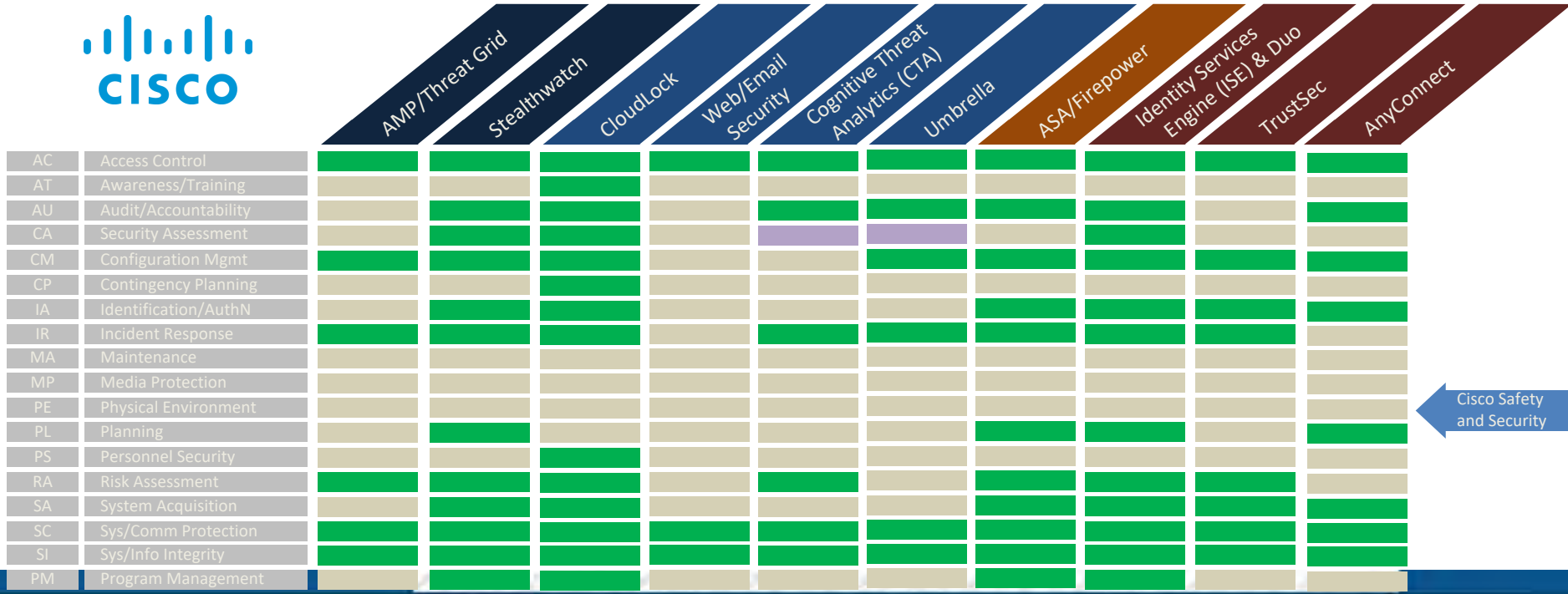
NIST CSF Alignment

Cisco Security Products

		AMP/Threat Grid	Stealthwatch	Cloudlock	Web/Email	Cognitive	Umbrella	Firepower	ISE & Duo	TrustSec	AnyConnect	Advisory	Implementation	Managed
ID	Access Management		■	■				■	■			■	■	■
	Business environment	Non-technical control area										■		
	Governance	Non-technical control area										■		
	Risk Assessment					■		■				■	■	■
	Risk Management	Non-technical control area										■	■	
	Supply Chain	Cisco Security and Trust Organization (S&TO)												
PR	Access Control		■	■			■	■	■	■	■	■	■	■
	Awareness Training	Non-technical control area										■		■
	Data Security	■	■	■	■	■	■	■	■	■	■	■		■
	Info Protection Process	Non-technical control area										■		■
	Maintanence										■	■		■
	Protective Technology	■						■	■	■	■	■		■
DE	Anomalies and Events	■	■	■	■	■	■	■				■		■
	Continuous Monitoring	■	■		■	■		■				■		■
	Detection Process	Non-technical control area										■		■
RS	Response Planning	Non-technical control area										■		■
	Communications	Non-technical control area										■		■
	Analysis	■	■	■	■	■	■	■				■		■
	Mitigation	■	■	■	■		■	■	■	■	■	■		■
	Improvements	Non-technical control area										■		■
RC	Recovery Planning	Non-technical control area										■		
	Improvements	Non-technical control area										■		
	Communications	Non-technical control area										■		

NIST SP 800-53

Cisco Solution Alignment Summary by Control Family

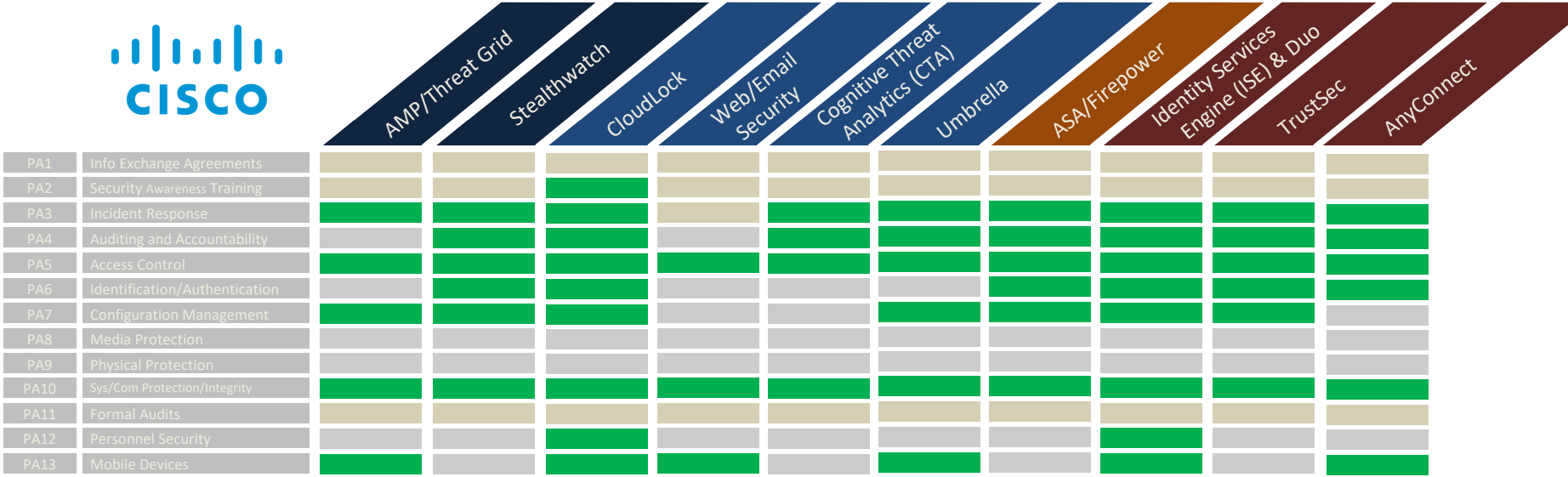


NIST SP 800-171

Cisco Solution Alignment Summary by Control Family

FBI CJIS Security Policy

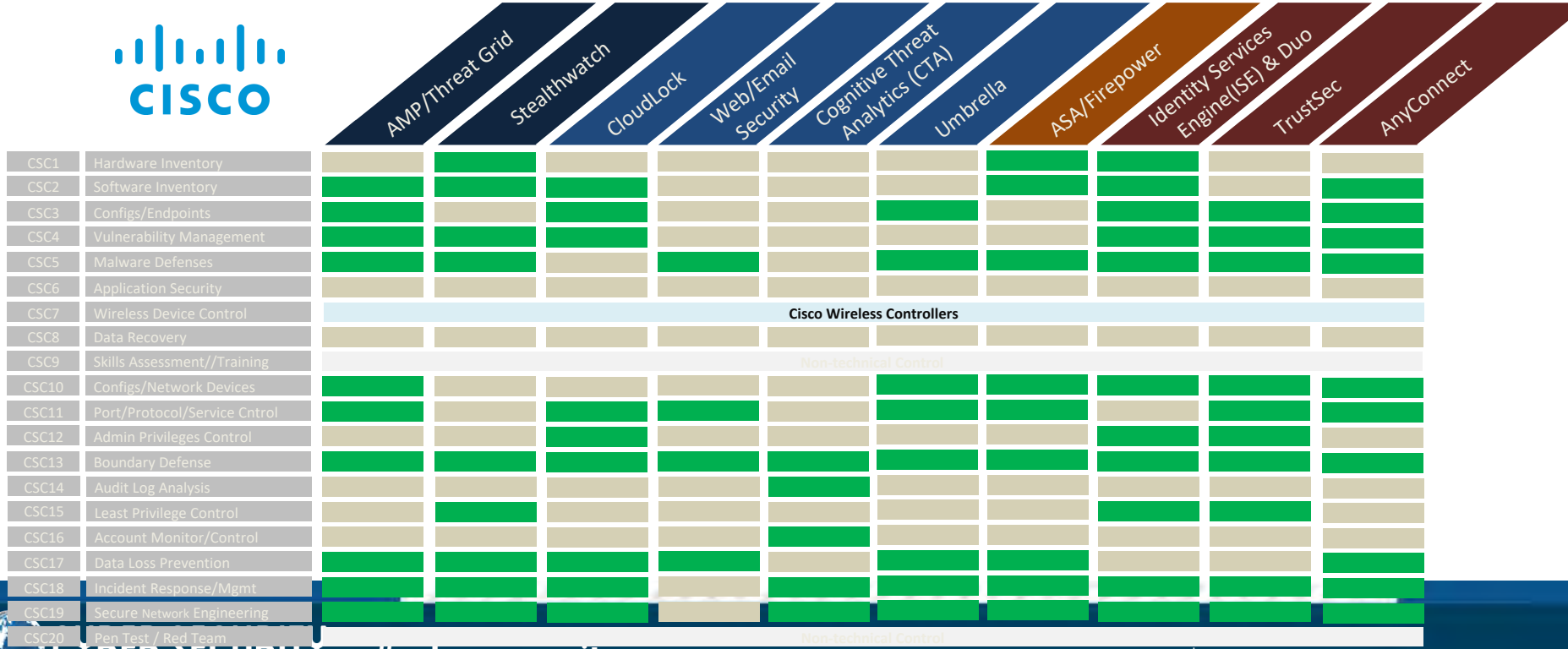
Cisco Solution Alignment Summary by Policy Area



CIS CSC

Center for Internet Security

Cisco Alignment Summary by Critical Security Control (CSC)



Thank You