
cisco Live!
ALL IN

The bridge to possible

Zero Trust Segmentation

From Theory to Implementation

Cindy Green-Ortiz, Cisco Senior Security Architect
CISSP, CSSLP, CISM, CRISC, PMP, CSM
@Sunburn9T and LinkedIn

BRKXAR-2008

Cisco Webex App

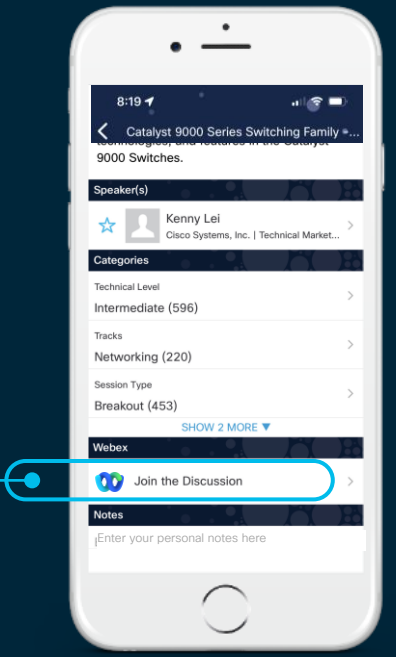
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



https://ciscolive.ciscoevents.com/ciscolivebot/# BRKXAR-2008

Cindy Green-Ortiz

- Global Enterprise Senior Security Architect @ Cisco for over 5 years, supporting Cisco Premier CXO Level Customers
- Leveraging 25+ years of experience in Security & Technology field across Financial, Healthcare, Hospitality, Public Sector, Manufacturing, Information Technology and Service Provider sectors
- Held many technology leadership roles, such as, DCIO, DCISO, Corporate Architecture and founded two technology businesses, writing a book on Zero Trust for Cisco Press
- Bachelor of Science in CIS Magna Cum Laude, Associate of Science CIS with Honors and currently holds the CISSP, CSSLP, CISM, CRISC, PMP, and CSM Certifications

Session Overview

Now that you know that you need to leverage a Zero Trust approach when segmenting your organization, what do you do now?

This session will cover an understanding of Zero Trust theory but will quickly move into what is needed to understand how to begin or continue implementation of zero trust segmentation in any organization and will enable anyone responsible for Zero Trust Segmentation to go back to their organizations with a broader and more in-depth understanding of where to start with Zero Trust Segmentation. Individuals will be able to define what is missing and how they're going to move their organization forward with the current landscape they have in place.

The speaker will go in-depth about these critical capabilities and use real-world examples of how implementation can go right, or how it can go very wrong, identifying pitfalls and ways to avoid them.

Agenda

Theory

Requirements

Design

Visualization

Implementation

Theory

Security Risk Landscape

Challenges → Access, Attack Surface, Visibility

Are they who they say they are?

Are devices secure & up to date?

What's on the network? How does it connect?

Excessive Trust

What data is in the cloud? Who/what accesses it?

How can we view & secure all connections?

What exists in the cloud? How does it connect? What tools are protecting the data?

TALOS

Security Guidance

Why do organizations need Zero Trust Segmentation?


Limit Compliance Scope & Attack Surface


Enable Rapid Service Deployment


Improve Network Stability and Resiliency


Long Term Cost Reductions


Protect Brand

"...there is not just one gate to the castle, but many, which has increased the attack vector significantly...cyber breaches can now occur not just through servers and ports, but through employee and third-party emails, devices and wireless connections."
– F. Lindstrom, KPMG

Value

People

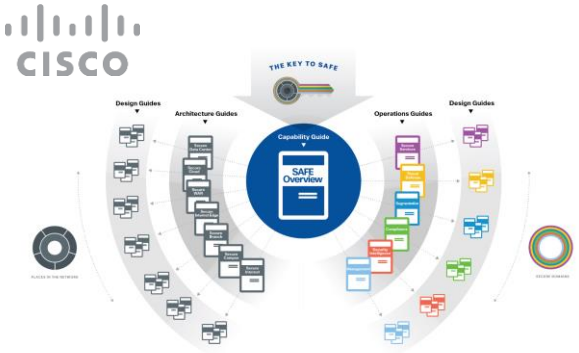
Process

Technology

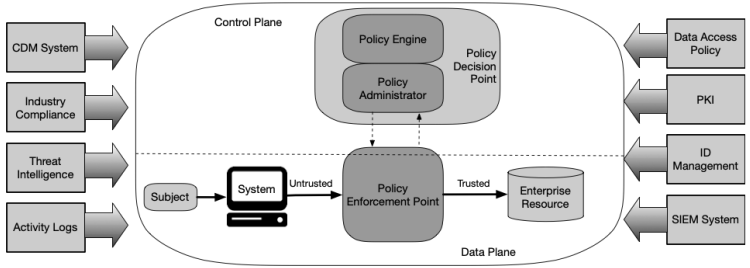
Common Drivers for Zero Trust Segmentation

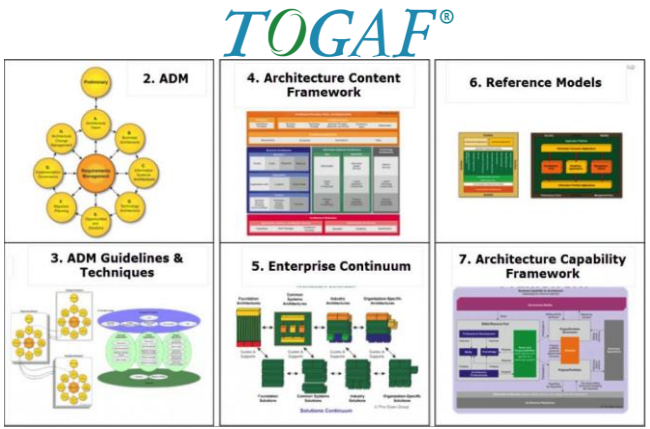
- Customers going through Merger & Acquisition activity
- Customers whose environments are understaffed or have high staff turnover
- Customers who have Flat / or almost Flat networks

Zero Trust Foundational Approach



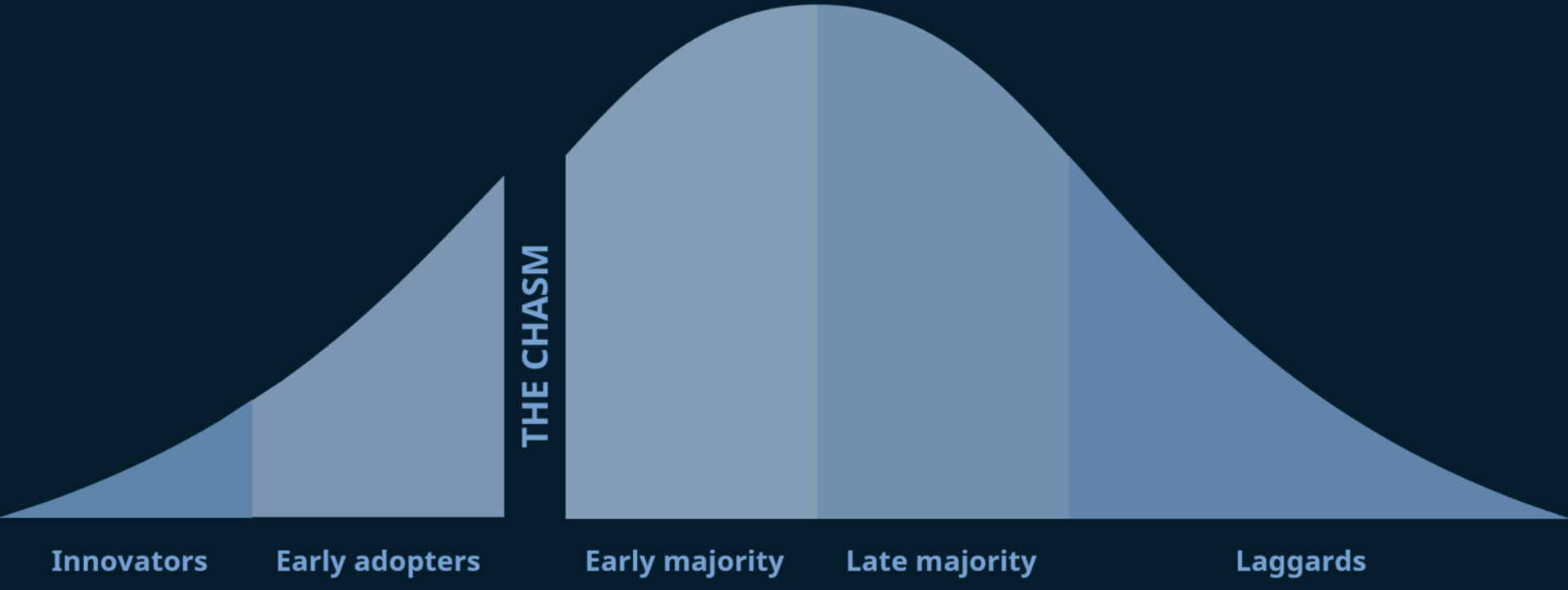
NIST Zero Trust Architecture 800-207





Requirements

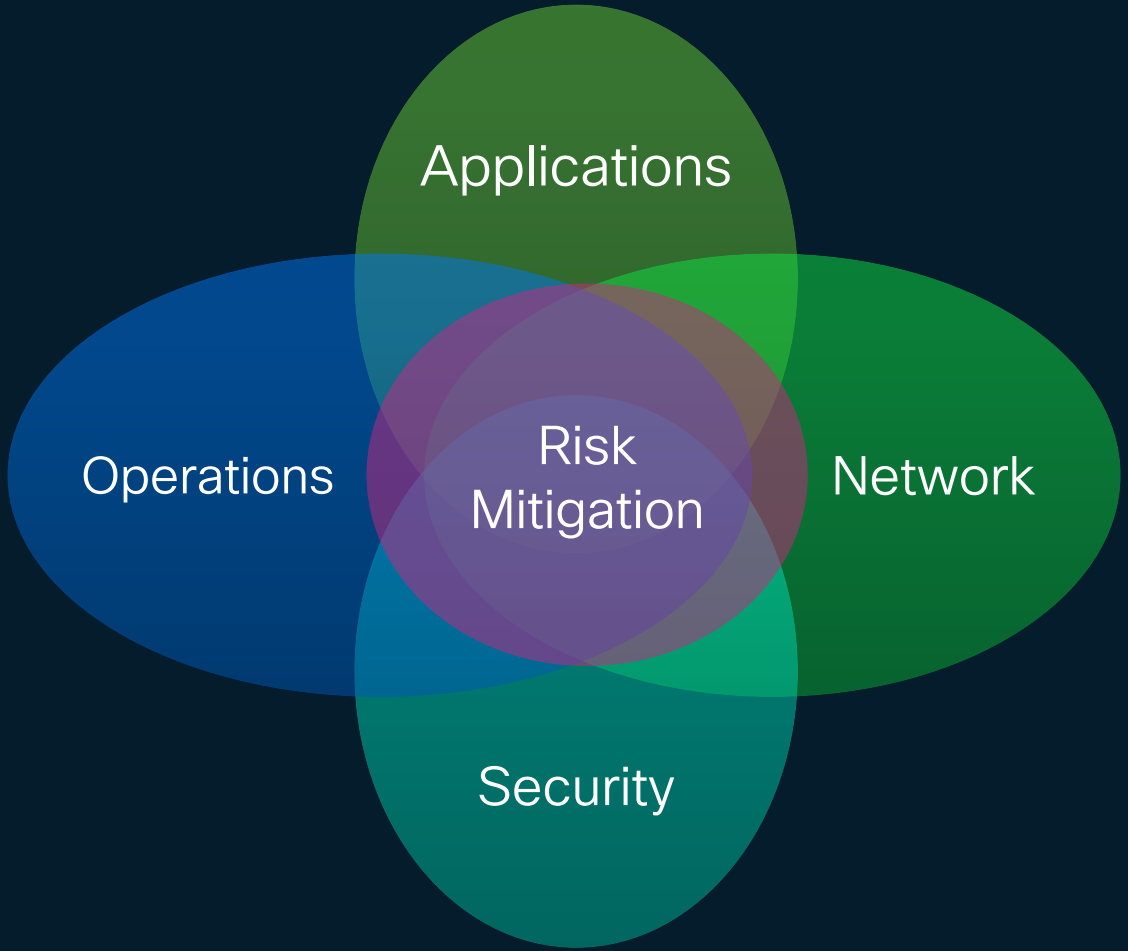
What is your Organization's Adoption Style?



*Technology Adoption Lifecycle from the book, "Crossing the Chasm," by Geoffrey A. Moore

Zero Trust Segmentation

Sample Organizational Ownership



Cisco's Zero Trust Capability Matrix

Identity

Vulnerability Management

Overlay

Enforcement

Analytics

Cisco's Zero Trust Capability Matrix

Identity

- AAA
- Certificate Authority
- NAC
- Provisioning
- Privileged Access
- MFA
- Asset Identity
- Configuration (CMDB)
- IP Schemas

Vulnerability Management

- Endpoint Protection
- Malware Prevention and Inspection
- Vulnerability Management
- Authenticated Vulnerability Scanning
- Database Change

Overlay

- Change Control
- Data Governance Policy
- Data Retention Policy
- QoS
- Redundancy / Replication
- Business Continuity
- Disaster Recovery
- Risk Classification Policy

Enforcement

- CASB
- DDoS
- DLP
- DNS Security
- Email Security
- Firewall
- IPS
- Proxy
- VPN / RA
- SOAR
- File Integrity Monitor

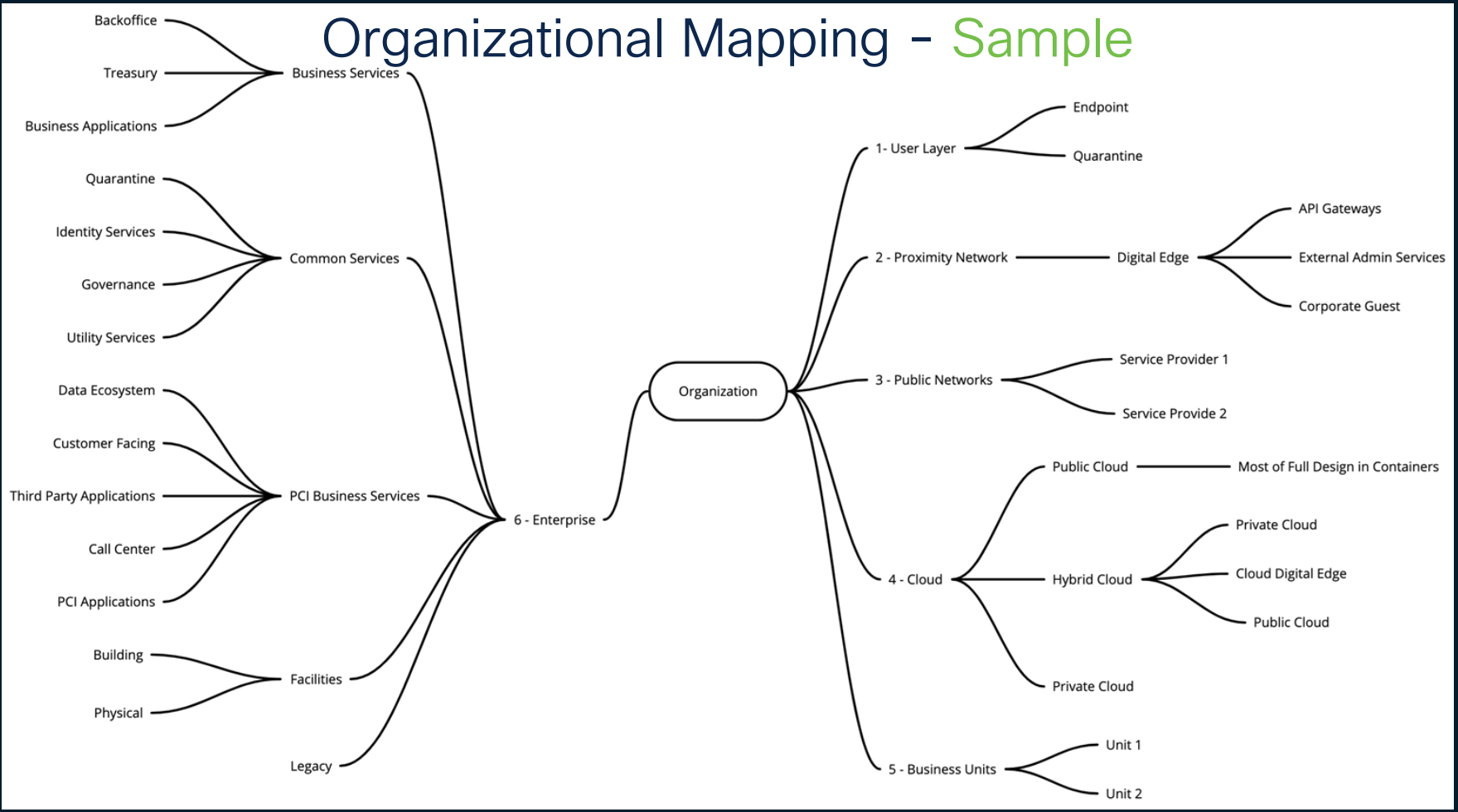
Analytics

- APM
- Audit, Logging, and Monitoring
- Change Detection
- Network Threat Behavior Analytics
- SIEM
- Threat Intelligence
- Traffic Visibility
- Asset Monitoring & Discovery

Matrix Developed by Cisco Security Services

Design

Organizational Mapping - Sample



Zero Trust Segmentation - Readiness Scorecard

Overall Readiness

Mitigation Priorities:

Identity

Needs Review

Needs Improvement

Missing

Vulnerability Management

Needs Review

Needs Improvement

Missing

Overlay

Needs Review

Needs Improvement

Missing

Enforcement

Needs Review

Needs Improvement

Missing

Analytics

Needs Review

Needs Improvement

Missing

CISCO SECURE

Security Reference Architecture

TALOS — Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt

Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) | ZERO TRUST

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

SDWAN

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Meraki Full Stack
- Secure Network Analytics
- Secure Web Appliance
- ISE TrustSec
- Cisco DNA Center

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

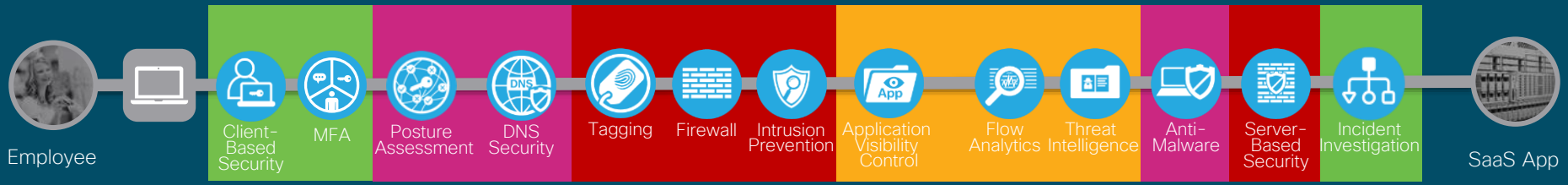
- Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

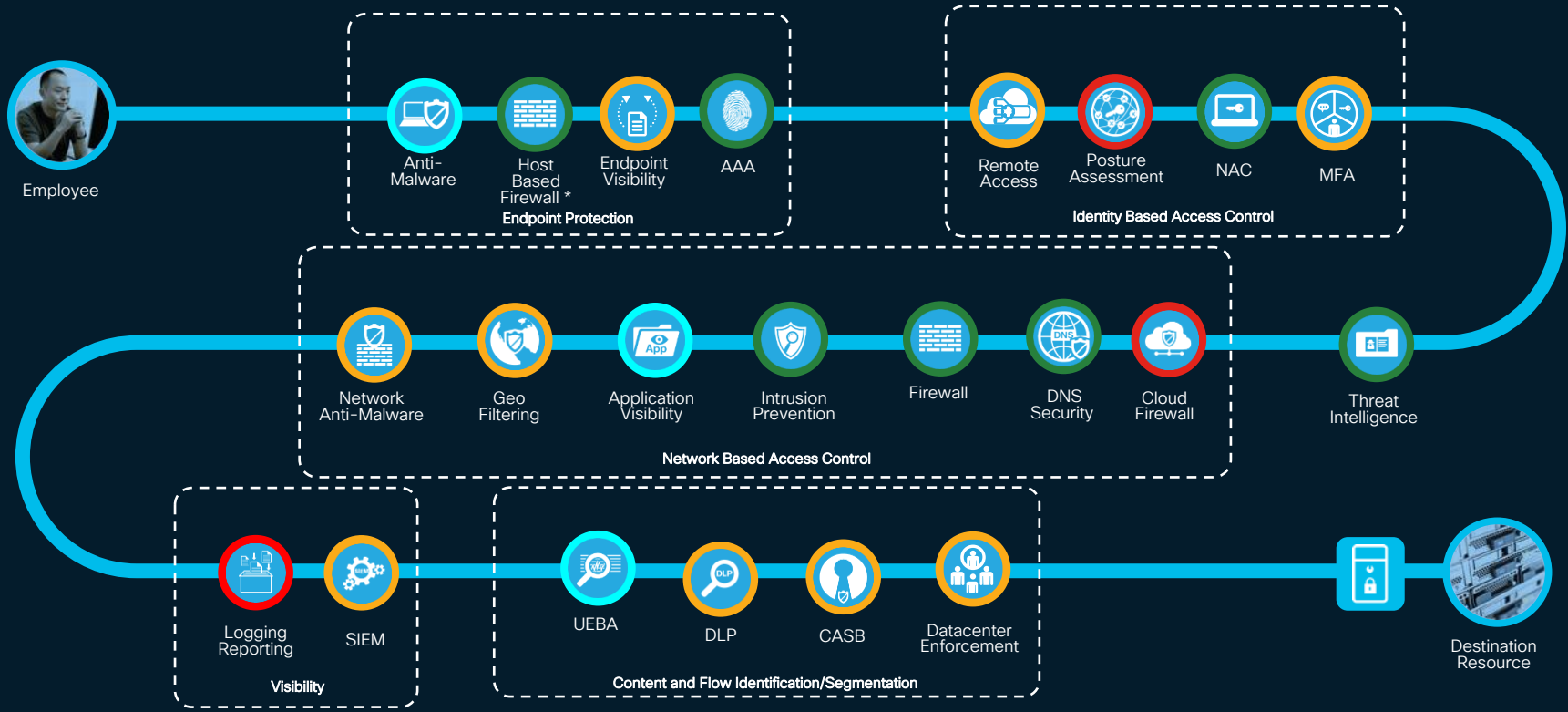
Zero Trust: Security – Threat Mitigation

Secure access to SaaS Applications: Employee accessing files in cloud storage



Identity | Vulnerability Management | Overlay | Enforcement | Analytics

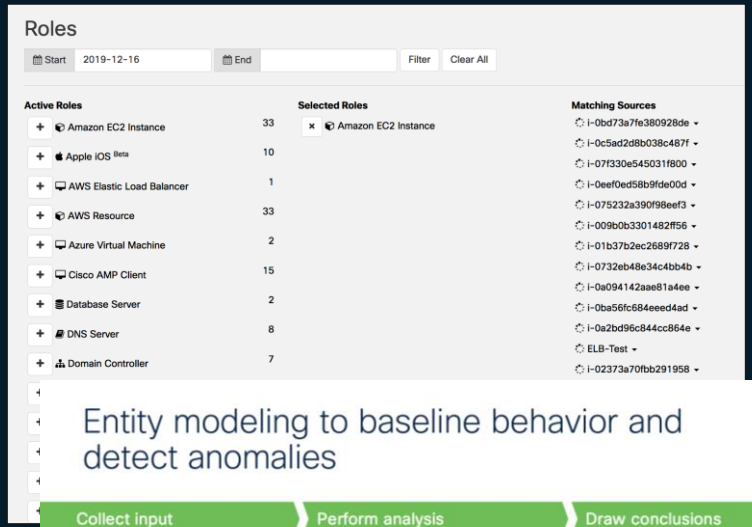
Zero Trust Capabilities – Sample Remote Worker Use Case

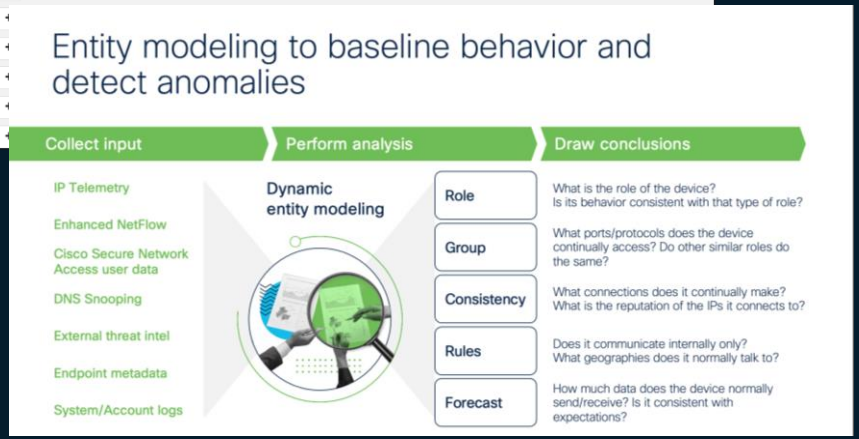


Visualization

Classify Device into Logical Segments - Using NetFlow

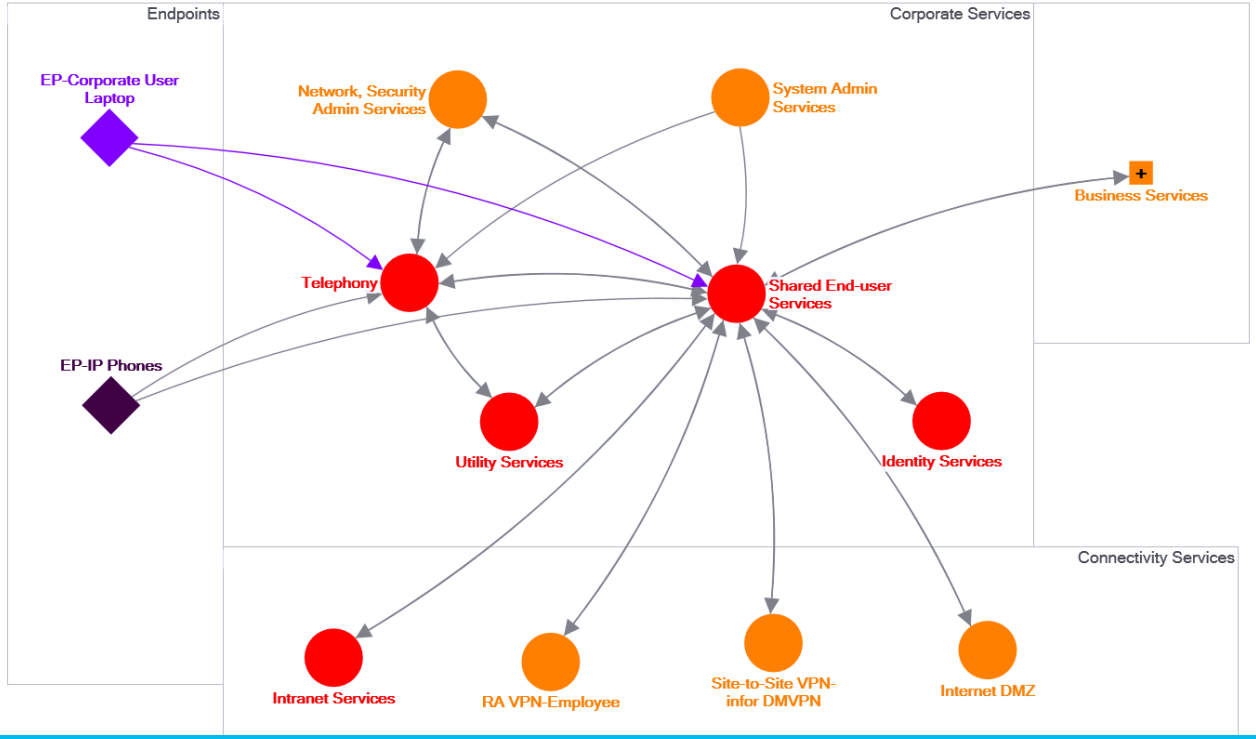
- Secure Network Analytics (formerly Stealthwatch) collects and analyzes network telemetry through a process called dynamic entity modeling that allows it to compare network behavior over time and generate alerts on any deviations from the expected behavioral norm.
- All types of devices and cloud resources are classified into roles, groups or segments
- We use NetFlow and cloud-native telemetry flow logs to learn about the behavior of assets in the cloud
- We also map existing data stores to further identify the device or workload





Zero Trust Segmentation: Application Flow

(via Secure Network Analytics and Cisco Tools)



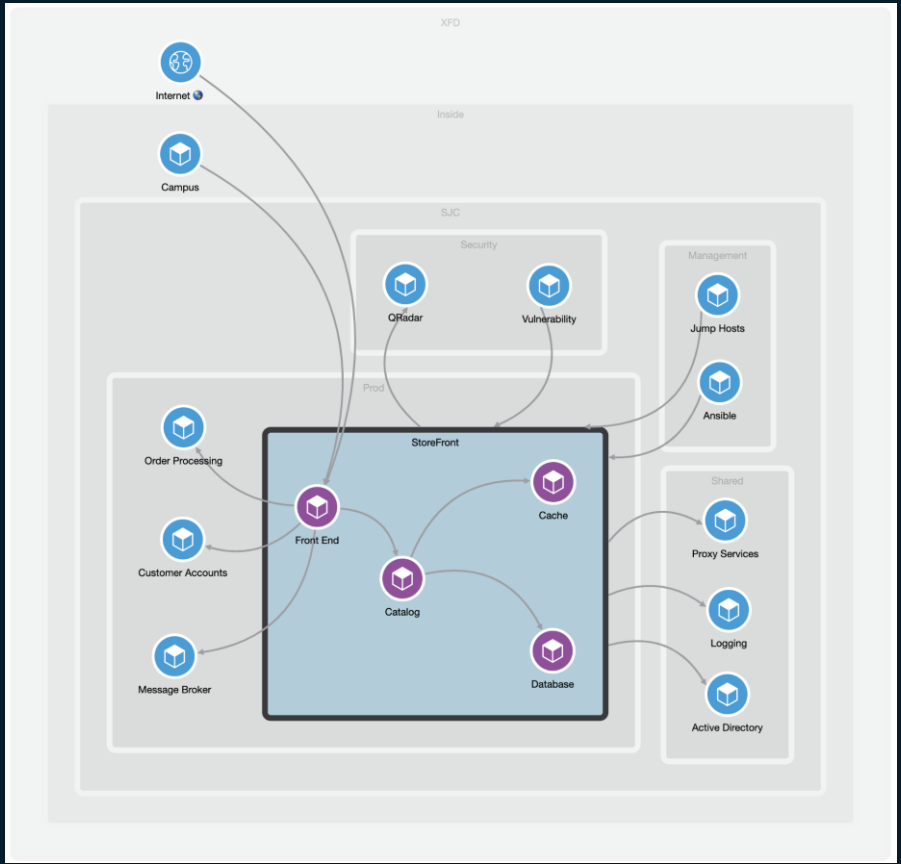
- Provides definition of the environment based on existing data sources (CMDB, Ticketing systems, etc.)
- Alerts when nefarious east – west activity occurs
- Provides Telemetry to other solutions

Zero Trust Segmentation - Application Enforcement

Ingestion of Secure Network Analytics information into Secure Workload helps map segments using automation

Then Secure Workload provides the blueprint and enforces controls for communication dependencies between application components as well as other IT services, mapped into the segments

- How are the different application tiers communicating?
- Are there direct connections coming to database servers?
- Which communication is going through load balancers?
- Are there connections going out that should not be allowed?



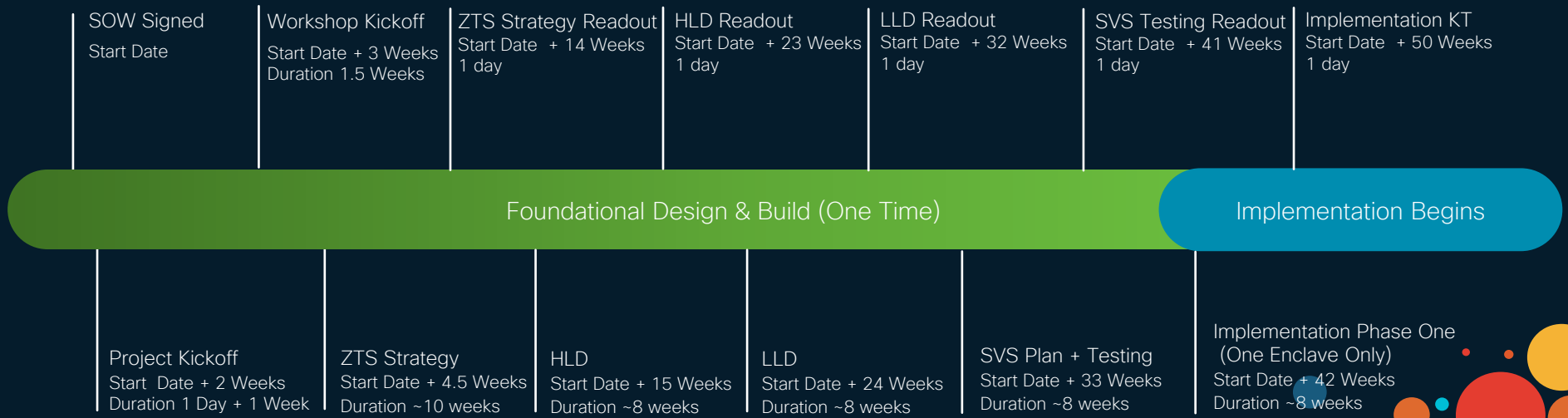
“Perfect is the enemy of good”

- Voltaire

Please remember to complete the survey for this session

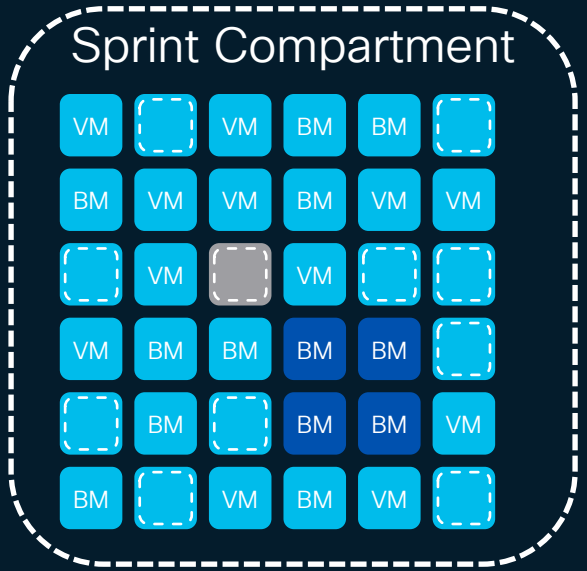
Implementation

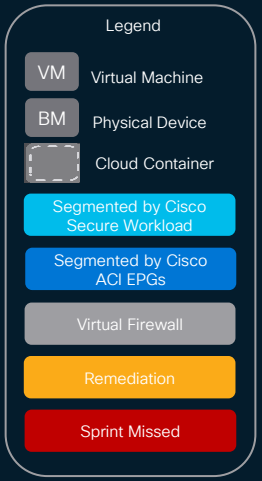
Zero Trust Segmentation Schedule – Typical



Zero Trust Segmentation – Workload Enforcement Sprint

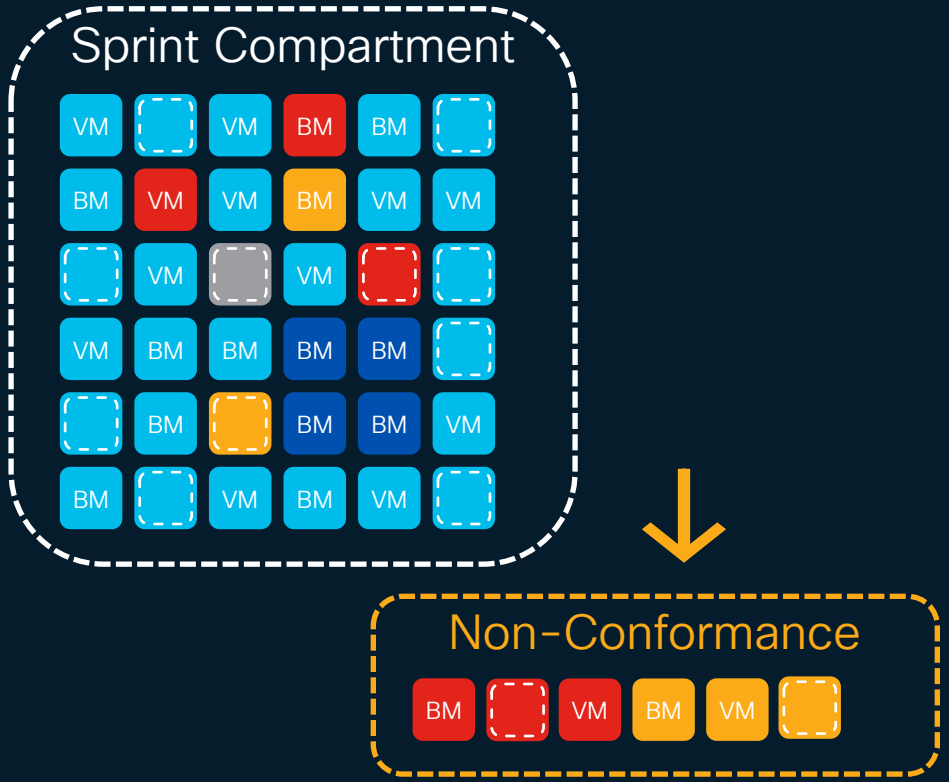
Example – Typical Enforcement Model





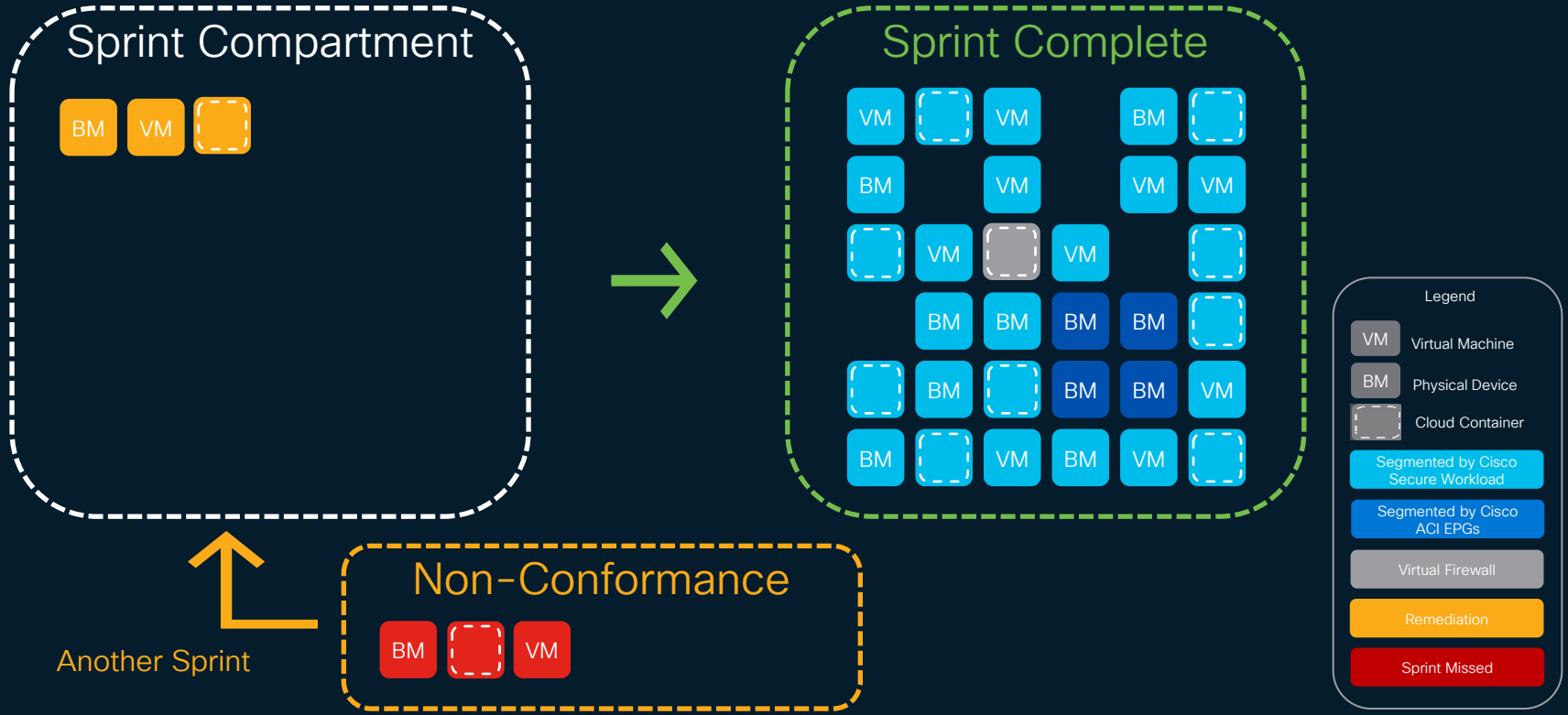
Zero Trust Segmentation – Workload Enforcement Sprint

Example – Typical Enforcement Model



Zero Trust Segmentation – Workload Enforcement Sprint

Example – Typical Enforcement Model



Zero Trust Segmentation – Implementation + Enforcement

Build Implementation Program Governance

Develop Application Owner Onboarding Process

Prep the Sprints and Sprint Workload Owners

Develop Policy (Global + Specific to Use cases)

Implement Enforcement

Post Implementation Knowledge Transfer

Organizational Resource Recommendation - Assign (18+) Stakeholders:

- 1+ Sponsor
- 1 Program Manager (FTE)
- 2 Secure Workload Leads (FTE)
- 2 Network Operations Leads (FTE)
- 2 Applications Lead (FTE),
- 2 Security Lead (FTE),
- 8 Supporting resources (PT)

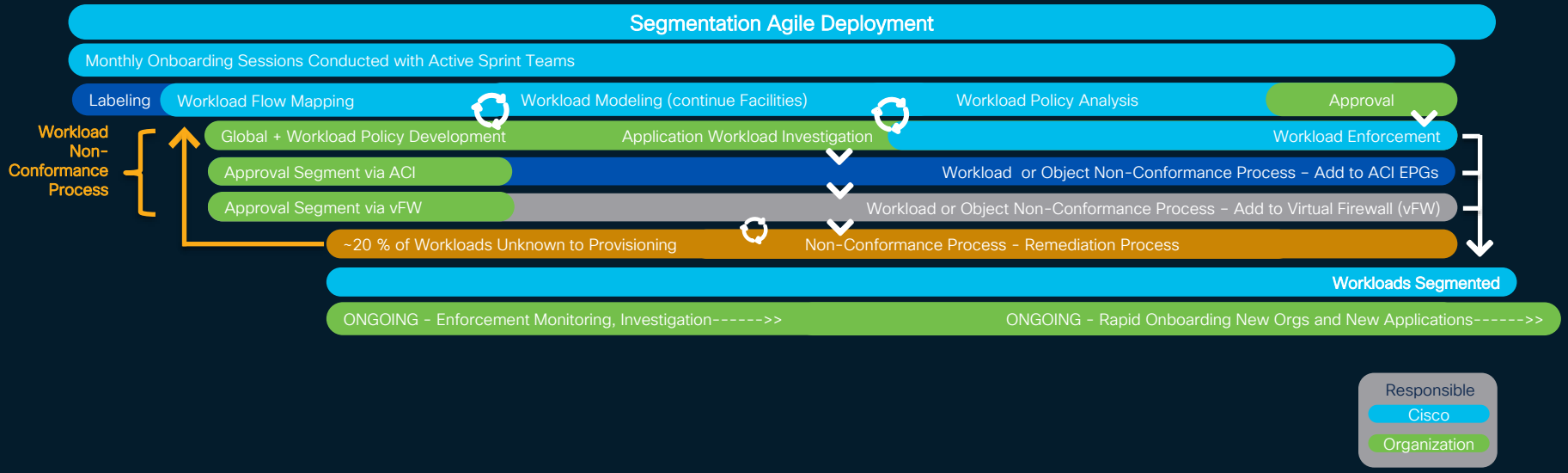
Zero Trust Segmentation – Agile Deployment

Approval Process
Duration:
20 Days

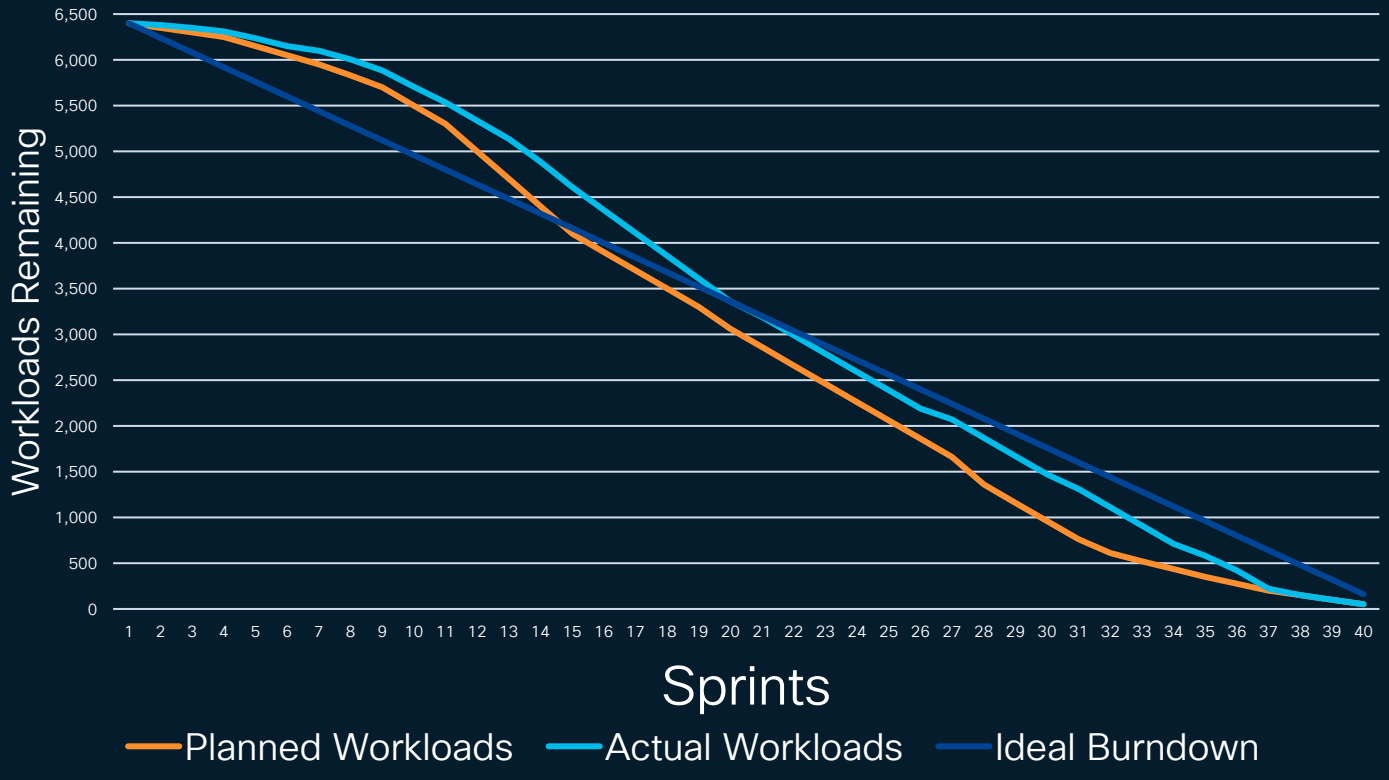
Workload Flow Mapping, Policy Development
Date: Start
Duration: 60 Days

Workload Modeling, Policy Modification, Workload Investigation
Date: Start + 60 Days
Duration: 90 Days

Workload Policy Analysis, Workload Enforcement, Non-Conformance Process, Remediation
Date: Start + 150
Duration: + 200 Days +



Zero Trust Segmentation - Burndown Chart



Key Assumptions & Requirements

- 40 Sprints over 10 months
- 2 Week Sprints
- Documented and enforced Escalation Process for Remediation

Workstreams

- Secure Workload (Tetration) Segmentation
- ACI EPG Migration
- Virtual Firewall Integration
- Non-Conformance Process Remediation (including delays)

Governance

- Governance across all workload owners (NetOps, DevOps, SecOps, App Owners)

In Summary


Create a Mind Map of Organization
Create the End State Segmentation Design
Trust Mapping
Define Zero Trust Protection Gaps
Build NetFlow Segmented Base Map
Tag Hosts to All Segments
Begin Enforcement

Questions?

Learn more in our upcoming book titled “Zero Trust: From Theory to Implementation” later this year

Please remember to complete the survey for this session

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

Thank you


cisco Live!
ALL IN