Cisco CISO Day I Barcelona I January 27 2020

Zero Trust

What does it means and how to get started

Richard Archdeacon

Advisory CISO EMEAR

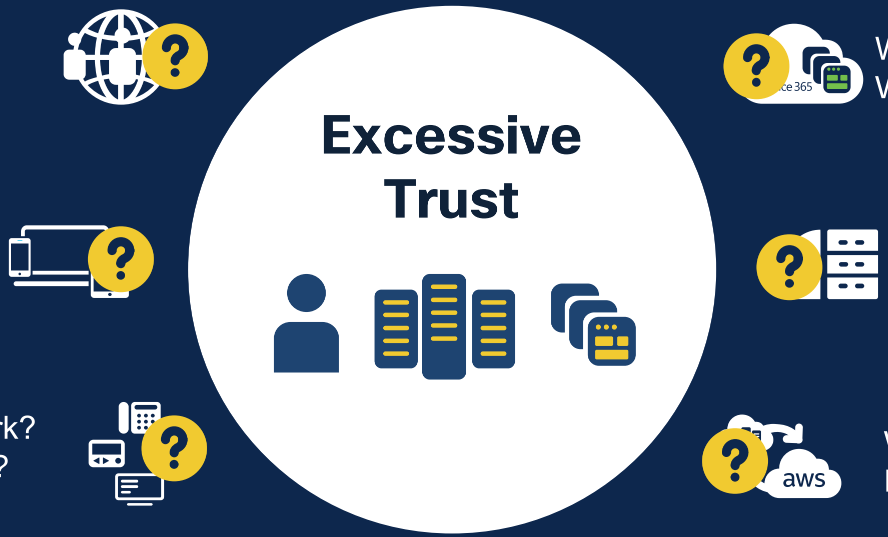
Topics for discussion

- Why do we need Zero Trust
- The history of Zero trust
- Cisco and Zero Trust
- Lessons learned

Never Trust – Always Verify

Business Challenges

Increased access, attack surface & gaps in visibility



How do we know users are who they say they are?

Are their devices secure & up to date?

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

What data's in the cloud? Who/what accesses it?

How can we view & secure all connections?

What exists in the cloud? How does it connect?

“Hackers don’t break in anymore they just login”.

CISO Major Technology company

“I want to get the basics right – know my inventory, what patch levels my devices have and get my Active Directory right. Once I have these under control I can concentrate on the other things”.

CISO Major Finance company

Seven factors in Digital Resilience

1. Prioritize information assets based on Risk
2. Provide differentiated protection for the most important assets
3. Integrate cyber security into enterprise wide risk management and governance processes
4. Enlist frontline personnel to protect the information assets they use
5. Integrate cyber security into the technology environment
6. Deploy active defences to engage attackers
7. Test continuously to improve incident response across business functions.

Beyond CyberSecurity - Kaplan, Bailey, Rezek, O'Halloran, Marcus

Threats Today, As a Result

A new approach to security is needed – zero trust – to address identity, app & network threats.

Targeting Identity

81% of breaches involved compromised credentials

Targeting Apps

54% of web app vulnerabilities have a public exploit available

Targeting Devices

300% increase in IoT malware variants

Secure how **someone** or **something** is accessing **work assets.**

SOMEONE

Employees
Contractors
Partners
Vendors
Auditors
Customers

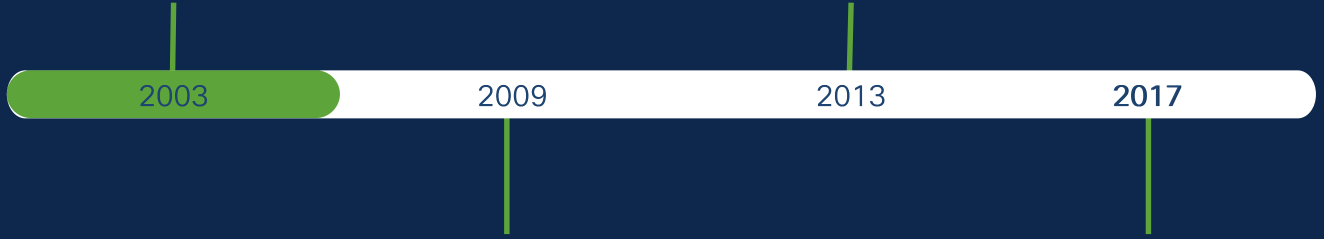
SOMETHING

IoT
APIs
Scripts
Printers
Cameras
Containers
Microservices
OT-equipment
Virtual machines
Medical equipment
Point-of-sale systems

WORK ASSETS

VPCs
Portals
APIs
Network
Servers
Databases
Containers
Applications
NW segment
Micro-services

Different Words - Similar Ideas



The Jericho Forum

First discusses

‘De-Perimeterisation’

John Kindervag

Forrester Analyst describes a

‘Zero Trust’ model

* Duo Security founded

First commercially available
Push Authentication

Google

Talk about their implementation

‘BeyondCorp’

Gartner Introduces ’CARTA’

Forrester Introduces ’ZTX’

* Duo Beyond

First commercially available
’Zero Trust’ Solution

What’s Different in a Zero-Trust Approach

The Traditional Approach

Trust is based on the network location that an access request is coming from.

→

Enables attackers to move laterally within a network to get to the crown jewels.

Doesn’t extend security to the new perimeter.

The Zero Trust Approach

Trust is established for **every access request**, regardless of where the request is coming from.

→

Secures access across your applications and network. Ensures only right users & devices have access.

Extends trust to support a modern enterprise with BYOD, cloud apps, hybrid environments & more.

Enabling Secure Access

Take a zero-trust approach to security to secure access across your entire IT environment.

Prevent Risks

Reduce risk of a breach before it happens

Gain Visibility

Identify risks and indicators of a breach of trust

Reduce Attack Surface

Contain breaches and stop attacker lateral movement

The Zero Trust Approach

Enable policy-based controls for every access request in a corporate environment

See who and what is accessing applications, workloads & the network

Segment your network & workloads by enforcing granular controls

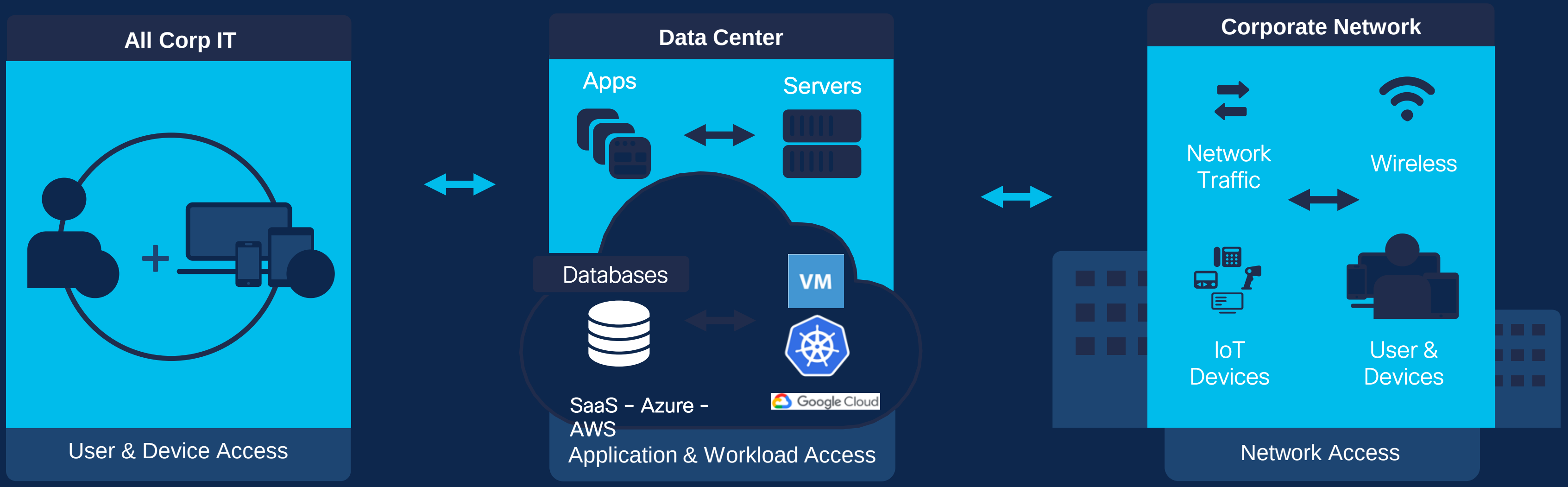
Securing Access

Access happens everywhere – how do you get visibility & ensure secure access?

Workforce

Workload

Workplace



All Corp IT

User & Device Access

Data Center

Apps

Servers

Databases

VM

Google Cloud

SaaS – Azure – AWS

Application & Workload Access

Corporate Network

Network Traffic

Wireless

IoT Devices

User & Devices

Network Access

Reducing the Risk - example

Threat	Vulnerability	Impact		Risk	
Attacker can access across the network and have a field day ↑	Intrusion through compromised credentials/ device ↑	Wide scale compromise - exfiltration, data corruption or system stoppage ↑	=	Widespread breach ↑	
Policy driven access and device checks reduce attack surface ↓	Trusted access reduces probability of password/ device compromise ↓	If device, user credentials, device check and policy fail - lateral movement limited ↓	=	Risk mitigated ↓	Zero Trust

How Cisco Verifies Trust

Establishing trust before granting access or allowing connections in your environment:

Workforce

+ Is the user who they say they are?

+ Do they have access to the right applications?

+ Is their device secure?

+ Is their device trusted?

Workload

+ What applications are used in the enterprise?

+ What is communicating with applications/data?

+ Is communication w/ the workload secure & trusted?

Workplace

+ Do users & devices authenticate for network access?

+ What access are they granted?

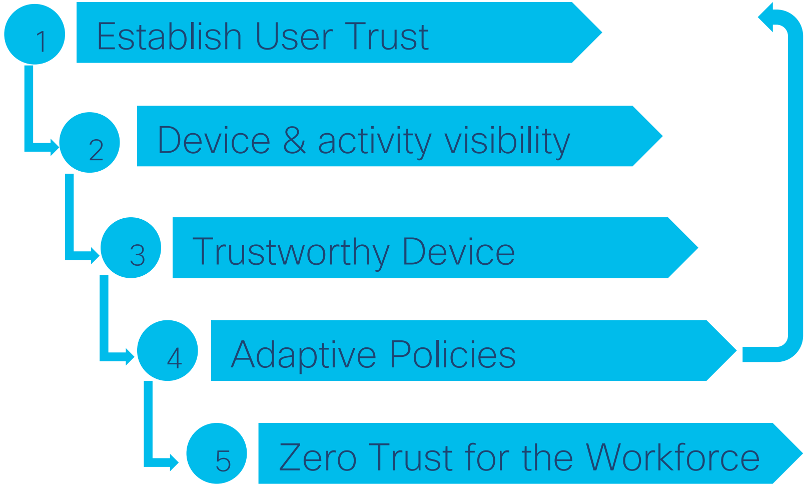
+ Are devices on the network secure?

+ Is their network segmentation based on trust?

So how do we start the change?

The Workforce

1. Find out and control the users with ease of use a priority
2. Understand how many devices are being used
3. Establish policy driven control around the status of devices
4. Implement policies matching the rules for access against the sensitivity of the data.
5. Monitor and respond to changes continuously

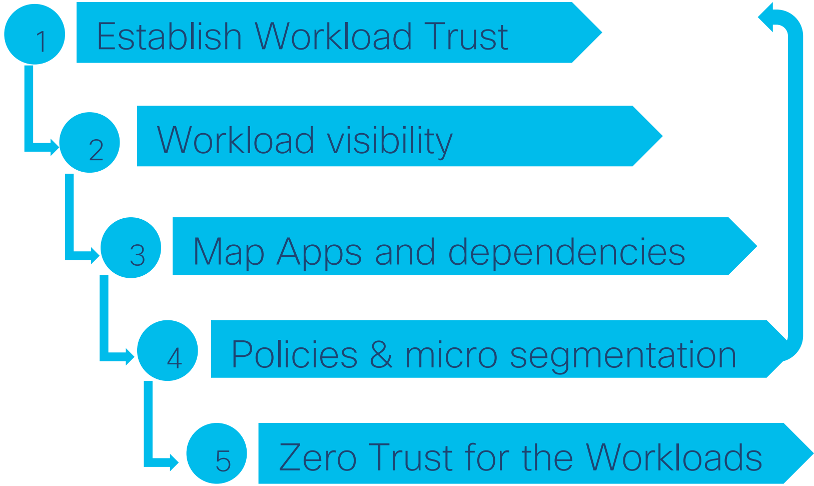


Lessons learned

1. Identify the stakeholders and user groups
2. Make it user centric
3. Define a clear set of KPIs
4. Maintain the momentum

The Workload

1. Understand the applications and mission critical workloads
2. Understand devices, process and how they communication within apps environment
3. Use comms and data flows to map application dependencies
4. Minimise trust through policies; reduce access perimeter
5. Monitor and respond to changes continuously

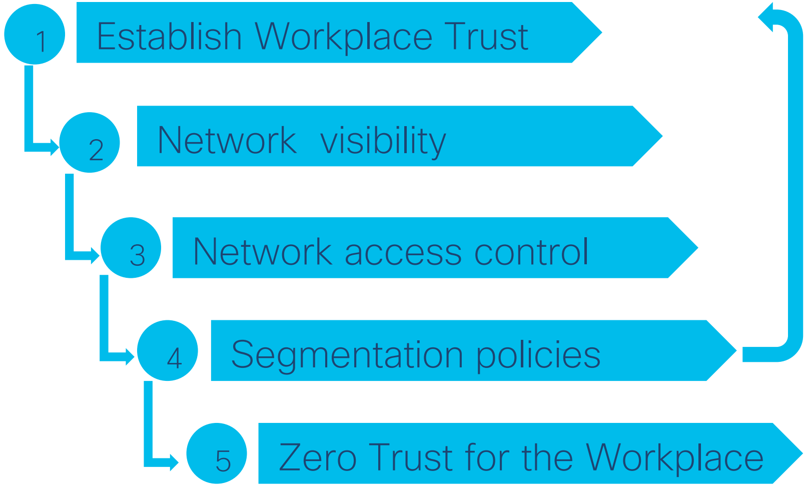

1
Establish Workload Trust
2
Workload visibility
3
Map Apps and dependencies
4
Policies & micro segmentation
5
Zero Trust for the Workloads

Lessons learned

1. Identify the apps and their owners
2. Make it app centric
3. Identify optimal working for apps
4. Maintain the process

The Workplace

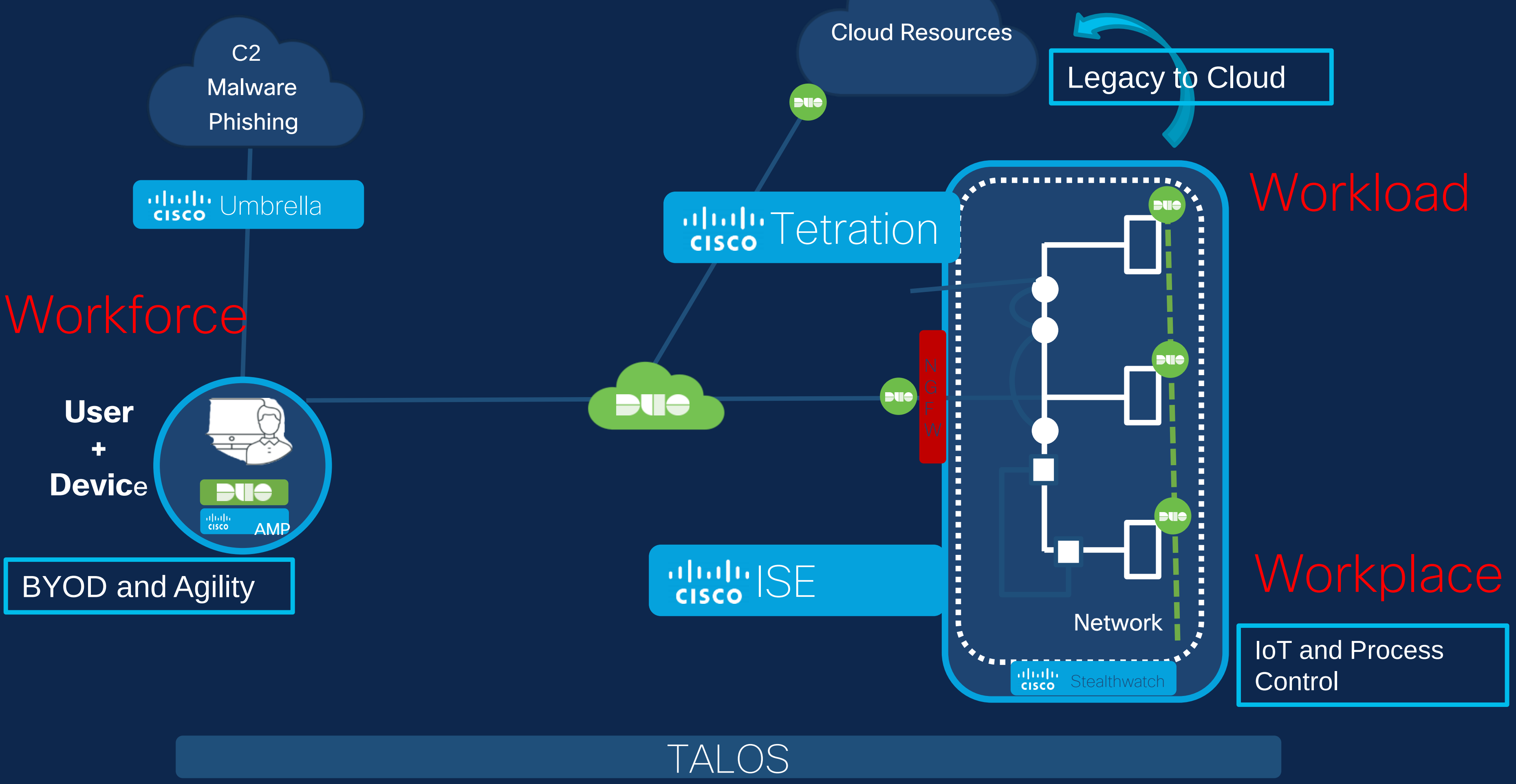
1. Discover devices and their owners including IoT/OT
2. Understand devices, process and how they communication within the workplace
3. Configure and enforce authentication and authorization for devices and equipment
4. Group based network policies ensuring controlled connections and comms
5. Monitor and respond to changes continuously



Lessons learned

1. Identify devices and inventory
2. Establish visibility
3. Define policies for access and segmentation
4. Maintain and monitor

Cisco Zero Trust



C2
Malware
Phishing

Umbrella

Workforce

User
+
Device

DUO

AMP

BYOD and Agility

Cloud Resources

Legacy to Cloud

Tetration

DUO

NGFW

ISE

Workload

Network

Stealthwatch

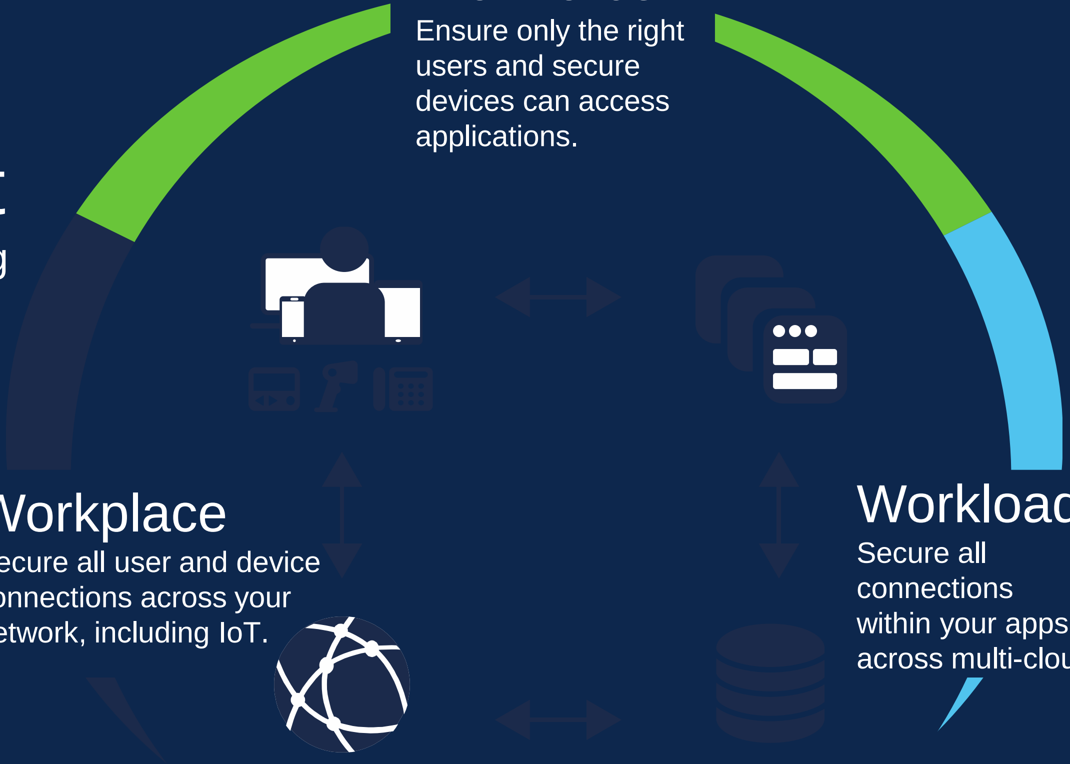
Workplace

IoT and Process Control

TALOS

Cisco Zero Trust

A zero-trust approach to securing access across your applications and environment, from any user, device and location.



Workforce

Ensure only the right users and secure devices can access applications.

Workplace

Secure all user and device connections across your network, including IoT.

Workload

Secure all connections within your apps, across multi-cloud.

Enforce policy based compliance

Summary on Zero Trust

- Is a way of thinking about how security is delivered
- Provides a basis to transform security to meet core challenges and demands
- Addresses account compromise, vulnerable equipment and application attacks
- Focus on Workforce, Workplace, Workload
- Every organization will have a different starting point
- Plan for an increased focus on policy and policy management
- Engage stakeholders to maintain momentum
- Look for technology integrations to provide flexibility

> “To improve is to change; to be perfect is to change often.”

Winston Churchill

Thank you